BANGALORE METRO RAIL CORPORATION LIMITED

Driving Bangalore Ahead

eTENDER DOCUMENT

FOR

Establishment, integration and Commissioning of On-premises "Security Operation Center" (SOC) for IT & CCTV Network of Bangalore Metro Rail Project and Operation & Maintenance of SOC for 3 years after Go Live

FOR

BANGALORE METRO RAIL CORPORATION LIMITED
Tender No. BMRCL/2025-26/SE0027

October–2025

BANGALORE METRO RAIL CORPORATION LIMITED
III Floor, BMTC Complex (C-Block), K H Road, Shanthinagar
Bengaluru– 560 027 Karnataka
India

PAGE INTENTIONALLY LEFT BLANK

KEY DETAILS

Tender No. BMRCL/2025-26/SE0027 *(BMRCL's File no. BMRCL/IT&CCTV/03/2023)*		
Name of Work: Establishment, integration and Commissioning of On-Premises "Security Operation Center" (SOC) for IT & CCTV Network of Bangalore Metro Rail Project and Operation & Maintenance of SOC for 3 years after completion of go live		
Sl.no.	**Description**	
1.	Tender Security / EMD Amount	**INR 6,99,200/-** (Indian Rupees Six Lakh Ninety-nine Thousand Two Hundred only)
2.	Completion period of Works	42 Months
3.	Download of Tender documents	Tender documents to be downloaded from Karnataka Public Procurement Portal (eProcurement Portal: https://kppp.karnataka.gov.in/)
4.	Last Date of Seeking Clarification	As per Date and Time specified in e-Procurement Portal.
5.	Pre-bid meeting	As per Date and Time specified in e-Procurement Portal.
6.	Date and Time of submission of Tender	As per Date and Time specified in e-Procurement Portal.
7.	Date and Time of opening of Tender (Qualification cum Technical Package)#	As per Date and Time specified in e-Procurement Portal.
8.	Date and Time of opening of Tender (Financial Package)	Will be intimated to the Qualified Tenderers through e-Procurement Portal. Tenderers to trace the same.
9.	Place of Opening of Tenders (Qualification Cum Technical Package & Financial Package)	Office of the Managing Director Bangalore Metro Rail Corporation Ltd 3rd Floor, BMTC Complex (C-Block) K H Road, Shanthinagar Bangalore, PIN:560027 Karnataka, India
10.	Address for communication	Office of the Managing Director Bangalore Metro Rail Corporation Ltd., 3rd Floor, BMTC Complex (C-Block) K H Road, Shanthinagar Bangalore, PIN: 560027 Karnataka, India. Ph No: 080-22969300 Fax No: 080-22969222 Email: cylesh@bmrc.co.in

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Section No.	Description	Page No.
1	NOTICE INVITING TENDERS (NIT)	1
2	INSTRUCTIONS TO TENDERERS (ITT)	5
3	QUALIFICATION INFORMATION	25
4	FORM OF TENDER (FOT)	29
5	GENERAL CONDITIONS OF CONTRACT (GCC)	35
6	SPECIAL CONDITIONS OF CONTRACT (SCC)	55
7	TECHNICAL SPECIFICATIONS	59
8	DRAWINGS	95
9	PROFORMA OF BANK GUARANTEES	97
10	ANNEXURES	105
11	INSTRUCTIONS FOR COMPLETING THE PRICING DOCUMENT	117
12	PRICING DOCUMENT (BILL OF QUANTITY)	119

PAGE INTENTIONALLY LEFT BLANK

SECTION 1: NOTICE INVITING TENDERS (NIT)

NIT No.: _____ Date: _____

1. Bangalore Metro Rail Corporation Ltd (BMRCL) invites Tenders (Single stage – Two-cover System) from eligible Domestic Tenderers, registered in eProcurement Portal of Govt. of Karnataka (GoK), for the works detailed in the Table below

Tender No.	Name of the Works	EMD / Tender Security	Period of completion
(1)	(2)	(4)	(5)
As specified in e-Procurement Portal.	Establishment, integration and Commissioning of On-Premises "Security Operation Center" (SOC) for IT & CCTV Network of Bangalore Metro Rail Project and Operation & Maintenance of SOC for 3 years after completion of Go-live.	INR 6,99,200	42 months

Brief Scope of the work is provided in Instructions to the Tenderers (ITT) and the detailed description of Work is provided in Technical Specifications. Only 'Class-I Local Tenderers' and 'Class-II Local Tenderers' as defined under ITT clause 34 shall be eligible to bid. Purchase Preference to the 'Class-I Local Tenderer' shall be given who meets minimum Local Content as defined in ITT clause 34.

Only firm/s that/those is/are registered or incorporated in India is/are eligible to participate (or) Any Tenderer from a country, which shares a land border with India and to which the Govt. of India has not extended lines of credit or in which the Govt. of India is not engaged in development projects, will be eligible to bid in this Tender, only if the Tenderer is registered with the "Competent Authority', as defined in ITT clause 35.

2. **REGISTRATION**:

a) Tenders required to enroll on the Karnataka Public Procurement Portal (https://kppp.karnataka.gov.in/) by clicking on the link "Tenderers Registration" on the Karnataka Public Procurement Portal and by paying requisite registration fee.

b) As part of the enrolment process, the Tenderers will be required to choose a unique user name to assign a password for their accounts.

c) Tenderers are advised to register their valid email addresses and mobile numbers as part of the registration process. These would be used for any communication with the Tenderer.

d) Upon enrolment, the Tenderers will be required to register their valid Digital Signature Certificate (Only Class III Certificates with signing + encryption key usage) issued by any Certifying Authority recognized by CCA India.

e) Only one valid DSC should be registered by a Tenderer. Please note that the Tenderers are responsible to ensure that they do not lend their DSCs to others which may lead to misuse.

f) Tenderers then login to the website through the secured log-in by entering their user ID/password and the password of the DSC / e-Token.

g) The scanned copies of all original documents (as required) should be uploaded on portal in PDF/JPG format.

h) For any query regarding e-Procurement on the Karnataka Public Procurement Portal, contact helpdesk number: +91-80 4601 0000, +91-80 6894 8777, and Email ID: support@eprochelpdesk.com.

3. **SEARCHING FOR TENDERS/BIDS:**

Once the Tenderers have selected the proposal bids/tenders and if they are interested to participate, the Tenderers can pay non-refundable processing fee to Karnataka Public Procurement Portal.

However, the tenderer shall submit such transaction details along with their tender submission on e-Procurement portal. If the same transaction reference number has been submitted for more than one bid, all such bids shall be considered ineligible and summarily rejected.

It will be the responsibility of the Tenderer to check the website and see any Addendum /Corrigendum issued in this tender from time to time and ensure submission of Tender submittals accordingly.

4. Tender documents consist of the following Sections,

- Section 1 - Notice Inviting Tenders (NIT)
- Section 2 - Instructions to Tenderers (ITT)
- Section 3 - Qualification Information
- Section 4 - Form of Tender (FOT)
- Section 5 - General Conditions of Contract (GCC)
- Section 6 - Special Conditions of Contract (SCC)
- Section 7 - Technical Specifications
- Section 8 - Drawing
- Section 9 - Proforma of Bank Guarantees
- Section 10 - Annexures
- Section 11 - Instructions for completing Pricing Document.
- Section 12 - Pricing Document (Bill of Quantity) –as published in eProcurement portal.

5. Tenders must be accompanied by Tender Security/ Earnest Money Deposit (EMD) as specified in ITT clause 14, drawn in favour of "Bangalore Metro Rail Corporation Ltd'. Tender Security/EMD will have to be paid in full amount through online payment in e-Procurement Portal (or) submit in any one of the form of Electronic Bank Guarantee (eBG) or Bank Guarantee, payable & extendable at a designated branch in Bengaluru and shall be valid for 45 days beyond the validity of the Tender (i.e. 165 days from the date of submission of Tender).

6. Tenders must be submitted electronically through Karnataka Public Procurement Portal /eProcurement Portal (https://kppp.karnataka.gov.in/) before the last date & time prescribed in the e-Procurement portal using a valid DSC (Digital Signature Certificate).

All Tenderers are requested to note that the originals of those documents, as listed under ITT clause 9.2, should be submitted in hardcopy by 'Speed post' or 'in person' at BMRCL office within **5 days** from last date of Tender submission. Tender submission without such submission of original documents shall be liable for rejection.

7. Tenders cannot be submitted online after stipulated time of submission of Tender.

8. Tenders shall be valid for a period of **120 days** from the latest date of submission of Tenders.

9. 'Qualification cum Technical Package' will be opened as per the latest specified time and date published in the e-Procurement portal.

The Financial Packages of technically qualified Tenderers will only be opened at a date and time advised by BMRCL through e-Procurement Portal.

10. The Tenderer shall provide credentials in support of their eligibility, qualifying criteria, technical capability, financial strength/support and past work experience by supporting documents / client certificates / CA's audit reports set forth in ITT Clause 3.

11. The Employer requires that Tenderers and Contractors observe highest standard of ethics during the procurement and execution of the Contract. In pursuance of this policy, The Employer;

(a) will reject the Tender for the Work or rescind the Contract, if the Employer determines that the Tenderer / Contractor has engaged in corrupt or fraudulent practices.

(b) will declare a Contractor ineligible, either indefinitely or for a stated period of time, to be awarded a Contract, if the Employer, at any time, determines that the Tenderer or the Contractor has engaged in corrupt or fraudulent practices in competing for, or in executing, the Contract.

12. All Tenderers are hereby cautioned that Tenders shall be submitted without any deviation, alteration or modification. Tenders containing any deviation from contractual terms and conditions, specifications and other requirements shall be considered as non-responsive and shall be liable for rejection.

13. BMRCL reserves the right to accept or reject any or all Tenders in part or full without assigning any reason. No Tenderer shall have any cause of action or claim against BMRCL for rejection of his Tender.

14. Registered Tenderers with e-token are advised to frequently check the e-Procurement portal for any amendments like Addendum / Corrigendum.

15. BMRCL will not be held responsible for consequential damages/losses due to lack /interruption of power supply & internet, low speed of internet, System problems, loss of electronic information/data etc.

16. For further clarifications/details, contact: G.S. Cylesh ADGM(IT), BMRCL on +91 94482 87997, Fax-+91 080-2296 9222, E-mail: cylesh@bmrc.co.in

For any query regarding e-Procurement portal/ Tender submission, please contact helpdesk at+91-80-4601 0000, +91-80-6894 8777, Email: support@eprochelpdesk.com.

Managing Director
Bangalore Metro Rail Corporation Limited

PAGE INTENTIONALLY LEFT BLANK

SECTION 2: INSTRUCTIONS TO TENDERERS (ITT)

Table of Clauses

A. GENERAL **6**

1. DESCRIPTION OF THE WORK 6
2. ELIGIBLE TENDERERS 6
3. QUALIFICATION OF THE TENDERER 7
4. COST OF TENDERING 9

B. TENDER DOCUMENTS **9**

5. CONTENT OF TENDER DOCUMENTS 9
6. CLARIFICATION OF TENDER DOCUMENTS 9
7. AMENDMENT OF TENDER DOCUMENTS 10

C. PREPARATION OF TENDERS **10**

8. LANGUAGE OF TENDER 10
9. DOCUMENTS COMPRISING THE TENDER 10
10. FORM OF TENDER 11
11. TENDER PRICES 11
12. TENDER CURRENCY 12
13. TENDER VALIDITY 12
14. EARNEST MONEY DEPOSIT (EMD) / TENDER SECURITY 12
15. FORMAT AND SIGNING OF TENDER 13

D. SUBMISSION OF TENDERS **14**

16. SEALING AND MARKING OF TENDERS 14
17. DEADLINE FOR SUBMISSION OF THE TENDERS 15
18. LATE TENDERS 15
19. MODIFICATION AND WITHDRAWAL OF TENDERS 15

E. TENDER OPENING AND EVALUATION **16**

20. TENDER OPENING 16
21. PROCESS TO BE CONFIDENTIAL 17
22. CLARIFICATION OF TENDER SUBMITTALS 17
23. EXAMINATION OF TENDERS AND DETERMINATION OF RESPONSIVENESS 17
24. CORRECTION OF ERRORS 18
25. EVALUATION AND COMPARISON OF TENDERS 18

F. AWARD OF CONTRACT **19**

26. AWARD CRITERIA 19
27. EMPLOYER'S RIGHT TO VARY QUANTITIES DURING THE CONTRACT 19
28. EMPLOYER'S RIGHT TO ACCEPT ANY TENDER AND TO REJECT ANY OR ALL TENDERS 19
29. NOTIFICATION OF AWARD AND SIGNING OF AGREEMENT 19
30. SECURITY DEPOSIT / PERFORMANCE SECURITY 19
31. CORRUPT OR FRAUDULENT PRACTICES 20
32. ONE TENDER PER TENDERER 20
33. SITE VISIT 20

G. PREFERENCE TO MAKE IN INDIA **20**

34. LOCAL CONTENT & PURCHASE PREFERENCE 20
35. ELIGIBLE SOURCE COUNTRIES OF THE TENDERER 22

SECTION – 2 : INSTRUCTIONS TO TENDERERS

A. GENERAL

1. Description of the work

Bangalore Metro Rail Corporation limited (BMRCL), a Special Purpose Vehicle (SPV) established under the Companies Act, 1956 (hereinafter referred to as "BMRCL" or "the Company" or "the Employer" or "the Client"), invites Tenders following **Single stage - Three Cover Tender procedure**, from the eligible Tenderers for "Establishment, integration and Commissioning of On-Premises "Security Operation Center" (SOC) for IT & CCTV Network of Bangalore Metro Rail Project and Operation & Maintenance of SOC for 3 years after completion of go live" (hereinafter referred to as "the Works") as per terms and conditions contained in this Tender documents.

2. Eligible Tenderers

2.1 Tenderers shall not be under a declaration of ineligibility for corrupt and fraudulent practices issued by the Government of Karnataka or BMRCL.

2.2 The Tender can be submitted by a firm registered under the Companies Act, 1956/2013 or Partnership firm registered under the Partnership Act of 1932 or registered (Converted 2013 to) under the Indian Limited Liability Partnership Act, 2008 (this is applicable for each member in case of a Joint Venture /Consortium).

2.3 The Tenderer may be a company (Private, Joint or Government owned) or any combination of such entities in the form of a Joint Venture/Consortium under an existing agreement or with the intent to enter into such an agreement supported by Letter of Intent.

In case, the Tenderer is a Joint Venture/ Consortium:

a all members shall be **jointly and severally liable** for the execution of the Contract in accordance with the Contract terms,

b shall nominate a Leader (member-in-charge) who shall have the authority to conduct all business for and on behalf of any and all the members of the JV/ Consortium during the Tendering process and in the event the JV/ Consortium is awarded the Contract, during Contract execution.

c the Leader shall be authorized to incur liabilities, receive payments and receive instructions for and on behalf of any or all members of the Joint venture/Consortium.

d shall submit complete details of the proposed division of role, responsibilities and corporate relationships among the individual members, indicating their **percentage of participation**.

e maximum number of members in the JV/ Consortium shall be **two (2),**

f shall submit a **notarized** Memorandum of Understanding (MoU) OR Consortium / JV Agreement OR Letter of Intent, comprising of all the members.

[In case it is notarized by the notary public of foreign country, the document shall be legalized by the Indian Embassy/High Commission. However, the document/s provided by a Tenderer from a country which has signed the 'Hague Legislation Convention 1961' is not required to be legalized by the Indian Embassy/High Commission if it carries a conforming "Apostille" certificate].

g Any change in composition of a Consortium or Joint Venture after submission of Tender will not be permitted and such Tender will be rejected.

h The **lead member** should be primarily responsible for entire IT network.

2.4 The Tenderer should not have been blacklisted / debarred by any Government / Government undertaking / semi Government / Govt. Controlled Institutions/projects in India, during last five (5) years. Also the Tenderer should not have rescinded the Works after award of the Contract during last five (5) years. The Tenderer shall provide an Undertaking as provided at Annexure-4.

Note: Last five (5) years shall be counted from 28 days prior to the date of submission of the Tender.

2.5 Only firm/s that/those is/are registered or incorporated in India is/are eligible to participate.

2.6 Only 'Class-I Local Tenderers' and 'Class-II Local Tenderers' as defined under ITT clause 34 shall be eligible to bid. Preference to the 'Class-I Local Tenderer' shall be given who meets minimum Local Content as defined in ITT clause 34.

3. Qualification of the Tenderer

Tenderers who meet the below specified minimum Qualification Criteria will only be qualified.

3.1 **Tender Capacity:**

Eligible Tenderers will be qualified only if their available Tender capacity is more than the total Tender value. The available Tender capacity will be calculated as under:

Assessed available Tender capacity = (A x N x 1.5 - B)

Where;

A = Maximum value of works executed in any one year during the last five years (updated to FY 2024-25 price level) taking into account the completed as well as works in progress.

N = Number of years prescribed for completion of the works for which Tenders are invited.

B = Value, at FY 2024-25 price level, of existing commitments and on-going works to be completed during the Contract Period of this Tender.

Note: *The statements showing the value of existing commitments and on-going works as well as the stipulated period of completion remaining for each of the works listed should be countersigned by the respective Employer-in-charge, not below the rank of an Executive Engineer or equivalent.*

3.2 **Financial Capabilities:**

3.3.1 **Average Annual Turnover**

i) In case of single entity:

The Tenderer shall have a minimum average annual turnover of **INR 139.83 Lakh** from the Works, calculated as total certified payments received from contracts in progress and/or completed within the last five (5) financial years divided by 5 years.

ii) In case of JV/Consortium:

a) All members combined shall have a minimum average annual turnover **of INR 139.83 Lakh** from the Works, calculated as total certified payments received from contracts in progress and/or completed within the last five (5) Financial years divided by 5 years, and

b) Lead member shall have a minimum average annual turnover of **INR 97.90 Lakh** from the Works, calculated as total certified payments received from contracts in progress and/or completed within the last five (5) Financial years divided by 5 years, and

c) Any member (other than Lead member) of the JV/Consortium shall have a minimum average annual turnover of **INR 14 Lakh** from the Works, calculated as total certified payments received from contracts in progress and/or completed within the last five (5) Financial years divided by 5 years.

3.3.2 **Liquidity**

i) In case of single entity:

The Tenderer shall demonstrate that it has access to or has available, liquid assets, lines of credit (Banker's certificate) sufficient to meet the cash flow requirements estimated as **INR 33.29 Lakh** for the subject contract.

ii) In case of JV/Consortium:

1. Any one member shall demonstrate that it has access to or has available, liquid assets, lines of credit (Banker's certificate) sufficient to meet the cash flow requirements estimated as **INR 16.65 Lakh** for the subject contract, and
2. All members combined shall demonstrate that they have access to or have available, liquid assets, lines of credit (Banker's certificate) sufficient to meet the cash flow requirements estimated as **INR 33.29 Lakh** for the subject contract.

Note:

1) *The last five (5) financial years shall be the last five (5) financial years ending 31st March, 2024 (i.e. FY 2019-20 to FY 2023-24).*
2) *Original Banker's certificate specifically for this work issued not earlier than 6 months from the date of submission of tender shall be submitted.*

3.3 **Work Experience:**

Tenderer either individually or jointly as a member of JV consortium should have an experience of carrying out "Similar Works", such as "implementation & Go Live of Security Operation Centre (SOC)" and should have successfully completed similar work during the last five (5) years ending 28 days prior to the last date of submission of tender and fulfill the following to establish the same:

i. The Tenderer should have executed at least One (01) similar work valued not less than INR 372.88 Lakhs; OR
ii. The Tenderer should have executed at least Two (02) similar works each of value not less than INR 233.05 Lakhs; OR
iii. The Tenderer should have executed at least Three (03) similar works each of value 186.44 Lakhs.

Note:

(1) Tenderer should submit necessary documentary evidence issued by the authorities (End user/Client's certificate/s) for successful Completion of the Work, failing which the Tender shall be rejected.

(2) Tenderer may be an OEM or its authorized agent/dealer/partner. In case the Tenderer is an Authorized agent/dealer/partner of any OEM, a valid "Authorization certificate" from the OEM shall be submitted.

3.4 All Tenderers shall provide the requested information accurately and in sufficient detail in **Section 3: Qualification Information**.

3.5 Subcontractors' experience and resources shall not be taken into account in determining the Tenderer's compliance with the qualifying criteria.

3.6 Even though the Tenderers meet the Qualification criteria in accordance with ITT Clause 3, they are subject to be disqualified if they have:

1. made misleading or false representations in the forms, statements and attachments submitted in proof of the qualification requirements; and/or

2. record of poor performance such as abandoning the works, not properly completing the Contract, inordinate delays in completion, litigation history, or financial failures etc.; and/or
3. Participated in the previous Tender for the same work and had quoted unreasonably high Tender prices and could not furnish rational justification.

4. Cost of Tendering

4.1 The Tenderer shall bear all costs associated with the preparation and submission of its Tender and BMRCL will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the Tender process.

4.2 The Tenderers shall be deemed to have inspected and examined the site and collected all necessary information regarding all factors and conditions likely to influence in carrying out the work, before uploading on e-Procurement portal and submitting his Tender.

B. TENDER DOCUMENTS

5. Content of Tender documents

5.1 Tendering procedures and Contract terms are prescribed in the Tender documents. The Tender document shall include:

1. Notice Inviting Tenders (NIT)
2. Instructions to Tenderers (ITT)
3. Qualification Information
4. Form of Tender
5. General Conditions of Contract (GCC)
6. Special Conditions of Contract (SCC)
7. Technical Specifications
8. Not Used
9. Proforma of Bank Guarantees
10. Annexures
11. Instructions for completing the Pricing document.
12. Pricing document (Bill of Quantity) – As published in eProcurement Portal.

5.2 The Tenderer is expected to examine all Instructions, Forms, Terms, and Specifications in the Tender documents. Failure to furnish all information required by the Tender documents or submission of a Tender not substantially responsive to the Tender documents in every respect will be at the Tenderer's risk and may result in rejection of its Tender.

6. Clarification of Tender Documents

6.1 Tenderers shall carefully examine the Tender documents and fully understand the conditions and matters, which may affect the work or the cost thereof. In case the Tenderer finds any discrepancies or omission from the specification or other documents, or in doubt as to their meaning, the Tenderer shall at once address query(ies) online through 'Karnataka Public Procurement Portal' (e-Procurement portal).

6.2 The Employer will offer clarification to such queries received through eProcurement portal up to the date specified therein.

Any such queries with details of clarification sought will be uploaded in the eProcurement portal (https://eproc.karnataka.gov.in) without disclosing the identity of the Tenderer seeking clarification. No separate future communication in this regard will be entertained.

6.3 While all efforts have been made to make the tender document error free, the Tenderer is advised to check the same carefully and may seek clarification(s) if any within the scheduled period only. No claims on account of any error(s), detected in the tender document, shall be entertained.

6.4 Pre-bid meeting:

6.4.1 The Tenderer or his authorized representative is invited to attend a Pre-bid meeting held at the Place, date and time indicated in Key Details/ eProcurement Portal.

6.4.2 The purpose of the meeting will be to clarify issues and to answer questions on any matter that may be raised at that stage to enable the Tenderers to submit Tenders without conditions.

6.4.3 The Tenderer is requested to submit any questions online through Karnataka Public Procurement Portal (e-Procurement portal) only, in terms of ITT clause 6.1.

6.4.4 Non-attendance at the Pre-bid meeting will not be a cause for disqualification of a Tenderer.

7. Amendment of Tender documents

7.1 At any time prior to the deadline for submission of Tenders, the Employer may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Tenderer, modify the Tender documents by an Addenda/Corrigenda.

7.2 Such Addenda/Corrigenda will be uploaded in the eProcurement portal. It will be the responsibility of the Tenderer to frequently check the eProcurement portal for any Addenda/Corrigenda or any other updates issued from time to time and ensure submission of Tender accordingly.

7.3 Without prejudice to the order of preference, the provisions in such addenda shall take priority over the Tender document issued previously. The Tenderers should acknowledge receipt of such addenda and list them in the tender submittals.

7.4 The Tenderer is not permitted to make any alteration /modifications to the Tender conditions. No modifications to the specifications, item descriptions, etc. will be entertained.

C. PREPARATION OF TENDERS

8. Language of Tender

8.1 The Tender prepared by the Tenderer, as well as all correspondence and documents relating to the Tender exchanged by the Tenderer and the Employer, shall be in English language. Supporting documents and printed literature furnished by the Tenderer may be in another language provided they are accompanied by an accurate translation of the relevant passages in the English language in which case, for purposes of interpretation of the Tender, the translated version in English shall govern.

9. Documents comprising the Tender

9.1 The Tender submittals shall comprise the following documents and Tenderer shall upload clear and readable scanned copies of these documents on e-Procurement Portal.

9.1.1 **Qualification cum Technical Package**

a) Earnest Money Deposit (EMD) /Tender Security (in accordance with ITT Clause 14);
b) The Form of Tender (in the format indicated in Section 4);

c) Qualification Information Form and Documents (in accordance with Section 3) and any other submissions as per requirements of Tender Document;
d) Covering Letter stating any other matter in relation to his tender which the Tender considers should be drawn to the particular notice of BMRCL.

and any other documents required to be completed and submitted by Tenderers in accordance with these instructions. **The documents listed under Sections 3 and 4 shall be filled in without exception.**

9.1.2 **Financial Package**

a) The Tenderer shall fill in and complete the Bill of Quantities (Financial Package) online through Karnataka Public Procurement Portal only and **no hardcopy of commercials should be attached or disclosed elsewhere.**
The Tenderer shall fill in and complete the Bill of Quantities in accordance with the 'Instructions for completing the Pricing Document', Section-11.

9.2 **Original Documents (Hardcopy):**

The Tenderer is required to submit the following documents in original (hard copy) within the time and place mentioned in ITT clause 16.7:

i) Tender Security/Earnest Money Deposit(EMD), as per clause 14,
ii) Notarized Power of Attorney and Board resolution (as applicable) as per ITT clause 15,
iii) Hardcopy of any other documents explicitly required in tender document.

In case of failure in submission of the above documents within stipulated date, the Tender may be treated as incomplete and be liable for rejection.

10. Form of Tender

The Tenderer shall complete the Form of Tender furnished in the Tender documents and submit duly signed (physically/digitally) along with the 'Qualification cum Technical Package'.

The Tenderer shall submit the priced 'Bill of Quantities' indicating the rate and amount with the 'Financial Package/Pricing Document' as published in eProcurement Portal.

11. Tender prices

11.1 The Contract shall be for the whole of the Works as described in Clause 1.0 of ITT, based on the priced 'Bill of Quantities' submitted by the Tenderer.

11.1.1 The quoted price shall be inclusive of all applicable Taxes, Cess and duties under the applicable Acts but **exclusive of GST** as specified under GCC Clause 39. The GST will be paid as applicable as per law.

11.1.2 The evaluation and comparison of Tenders shall be made accordingly by BMRCL. No claim will be entertained on this account after acceptance of the Tender or during the currency of the Contract.

11.1.3 **Income Tax (IT) deduction:** As per the prevailing rate, IT shall be deducted and remitted to the Income Tax authorities and Form 16 shall be furnished by BMRCL in proof of remittance to IT Department. For availing lower deduction of Income Tax, necessary certificate for each financial year issued by the Income Tax Authority shall be furnished by the Contractor, failing which IT at the maximum rate will be deducted.

11.2 The rates should be written in numerals (in figures and words) only. If the Tenderer indicates anything other than numerals, the Tender will be summarily rejected.

11.3 The rates and amounts quoted by the Tenderer shall be fixed for the duration of the Contract and shall not be subject to adjustment on any account, unless provided otherwise in the General/Special Conditions of Contract.

11.4 A Tender submitted with an adjustable price quotation will be treated as non-responsive and rejected, pursuant to ITT Clause 23.

12. Tender Currency

12.1 Prices shall be quoted in Indian Rupees only.

13. Tender validity

13.1 Tenders shall remain valid for a period as specified in 'Appendix to Form of Tender' (Section 4) after the deadline date for Tender submission specified in ITT Clause 17. A Tender valid for a shorter period shall be rejected by the Employer as non-responsive.

13.2 In exceptional circumstances, prior to expiry of the original time limit, the Employer may request that the Tenderers may extend the period of validity for a specified additional period. The request and the Tenderers' responses shall be made in writing or by cable. A Tenderer may refuse the request without forfeiting his Earnest Money Deposit. A Tenderer agreeing to the request will not be required or permitted to modify his Tender, but will be required to extend the validity of his Earnest Money Deposit for a period of the extension, and in compliance with ITT Clause 14 in all respects.

14. Earnest Money Deposit (EMD) / Tender Security

14.1 The Tenderer shall furnish, as part of its Tender, interest free Tender Security/ EMD as per eProcurement Portal.

14.2 The Earnest Money Deposit is required to protect the Employer against the risk of Tenderer's conduct which would warrant the security's forfeiture, pursuant to ITT Clause 14.8.

14.3 The Tenderer shall pay/furnish an EMD (Tender Security) for the value indicated in e-Procurement portal in the following mode:

a) online payment through eProcurement Portal,

or

b) an irrevocable Electronic Bank Guarantee (eBG) or Bank Guarantee, issued by an Indian Scheduled Bank (excluding Cooperative Banks) or by a Scheduled Foreign Bank as defined in Section 2(e) of RBI Act 1934 read with Second Schedule preferably drawn on and payable & extendable at a designated branch in Bengaluru in the form given in Proforma A of Section 9 to the Tender documents. 'Earnest Money Deposit' Bank Guarantee format is also available in https://tenderb.bmrc.co.in.

14.4 The Earnest Money Deposit shall be valid for a period as specified in 'Appendix to Form of Tender' (Section 4) and remain deposited with the Employer from the date of opening of Tenders. If the validity of the Tender is extended, the Earnest Money Deposit (EMD) shall also be duly extended, failing which, the Tender after the expiry of the aforesaid period shall not be considered by the Employer.

14.5 Tender Security/EMD will not be accepted in any form other than those mentioned above. Tenders not accompanied by the required amount of Tender Security/EMD and non-submission of hardcopy as per ITT clause 16.7 will be rejected by the Employer.

However, BMRCL reserves the right to accept or reject the Tender Security/EMD with any deficiency otherwise not materially affecting the technical qualification criteria of the Tenderer.

14.6 The Tender Security/EMD of unsuccessful Tenderers will be discharged/ returned upon the Successful Tenderer signing the Contract Agreement in pursuant to ITT clause 29.

14.7 The successful Tenderer's Earnest Money Deposit (EMD) will be discharged upon signing of the Contract Agreement by the successful Tenderer in pursuant to ITT clause 29 and furnishing the Performance Security pursuant to ITT Clause 30.

14.8 The Earnest Money Deposit (EMD) may be forfeited:

(a) If a Tenderer:
  (i) withdraws or amends or impairs or derogates its Tender during the period of Tender validity specified by the Tenderer on the 'Form of Tender'; or
  (ii) does not accept the correction of errors pursuant to ITT Clause 24.2; or

(b) In case of a successful Tenderer, if the Tenderer fails:
  (i) To sign the Contract Agreement in accordance with ITT Clause 29; or
  (ii) To furnish performance security in accordance with ITT Clause 30.

14.9 The Tender will be summarily rejected by the Employer in case of:

(i) Failure to deposit online EMD portion or failure to upload clear & readable copy of Bank Guarantee towards EMD.

(ii) Failure to submit the original Bank Guarantee /EMD to BMRCL office within the date & time specified,

(iii) If EMD(Tender Security) is in the form of Bank Guarantee and is issued by a co-operative bank or from any source other than an Indian Scheduled Bank and Scheduled foreign Bank as defined in section 2(e) of RBI Act 1934 read with Second Scheduled.

(iv) EMD (Tender security) amount is less than the required amount as mentioned in NIT.

(v) Bank Guarantee's Validity is less than Tender as mentioned in ITT clause 13.

In case EMD (Tender Security) is in the form of BG, and BG validity fulfils the "Tender validity Period", but falling short in regard to period of "EMD (Tender Security) Validity', the Employer shall request such Tenderer(s) in writing to submit compliant EMD (Tender Security) within 10 (ten) working days from the date of request. Failing to provide a compliant EMD (Tender Security), within the prescribed period, shall cause the rejection of the Tender and it will be considered as Non-responsive.

14.10 In case the Tenderer submits Electronic Bank Guarantee (e-BG), the UIN of BMRCL for providing e-BG shall be: AAACB4881D (PAN of BMRCL).

14.11 If the Tenderer has opted to submit the Tender Security in the form of Electronic Bank Guarantee (e-BG), a copy of the e-BG shall invariably be uploaded in eProcurement Portal.

15. Format and signing of Tender

15.1 The Tenderer shall follow and submit the Tender documents in the respective formats prescribed under Section 9-Proforma.

15.2 The Tender submittals shall be typed or written in indelible ink (wherever required), which is to be scanned and digitally signed using Class-III digital signature by person(s) duly authorized to bind the Tenderer to the contact. Proof of authorization shall accompany the Tender in the form of notarized "Power of Attorney". All pages of the Tender where entries, amendments, corrections, alterations, erasures etc., have been made shall be initialized by the person(s) signing the Tender.

15.3 The Tender shall contain no alterations or additions, except those to comply with instructions issued by the Employer, or as necessary to correct errors made by the Tenderer, in which case such corrections shall be initialed by the person signing the Tender.

15.4 Any individuals signing the Tender or other documents connected therein should specify whether he is signing:

(i) as sole proprietor of the firm or as attorney of the sole proprietor;

(ii) as a partner or partners of the firm;

(iii) as a Director, Manager or Secretary in the case of a limited company with a copy of Notarized Power of Attorney duly authorized by a resolution passed by the Board of Directors or in pursuance of the authority conferred by Memorandum of Articles of Association.

15.5 The original notarized 'Power of Attorney' or the documents empowering the individual or individuals to sign should be furnished to the Employer for verification, if required.

D. SUBMISSION OF TENDERS

16. Sealing and Marking of Tenders

16.1 All the Tender proposals shall be digitally signed along with the other Qualifying documents and shall be submitted Electronically through Karnataka Public Procurement Portal on or before the last date and time for Tender submission as published therein.

16.2 Tenderer, in advance, should get ready the Proposal documents to be submitted as indicated in the Tender document /schedule in PDF/JPEG formats. The Tenderer has to digitally sign and upload the required proposal documents one by one as indicated in the tender document.

16.3 Tenderer should log into the portal well in advance for the submission of the proposal so that it gets uploaded well in time i.e. on or before the last date & time for Tender submission.

16.4 Tenderer will be solely responsible for uploading the Tender submittals in eProcurement Portal. BMRCL will not be held responsible for consequential damages/losses/delays due to lack /interruption of power supply & internet, low speed of internet, System problems, loss of electronic information/data etc.

16.5 The server time (which is displayed on the dashboard) will be considered as the standard time for referring the deadline for submission of the proposals by the Tenderers, opening of proposals etc. The Tenderers should follow this time during proposal submission.

16.6 The necessary certificates/documents in support of fulfilling Eligibility Criteria and Technical requirements shall be scanned and attached to e-Procurement portal.

16.7 Original Documents to be submitted in hardcopy:

The Tenderer shall seal and submit the original documents listed in ITT clause 9.2 in original (hard copy) by speed post or in person at BMRCL office within 5 days of last date of online Tender submission. Only the tenders submitted online, the hardcopies will be considered for evaluation. The hardcopies should carry/accompany copy of acknowledgement from Employer/ eProcurement Portal".

The envelope shall bear the following identification:

TENDER NO: _____

ORIGINAL SUBMITTALS OF 'QUALIFICATION CUM TECHNICAL PACKAGE'

BMRCL Office Address for submission of hardcopy:

To

General Manager (IT)
Bangalore Metro Rail Corporation Ltd.,
3rd Floor (C-Block), BMTC Complex, K H Road,
Shanthinagar, Bengaluru - 560027, Karnataka.

The Tenderers can submit the hard copies by 'Speed Post' or 'in person' at the above address during 11.00 am to 05.00 pm on all working days. In case, 5th day happens to be holiday, then the next working day shall be considered as last day for submission of the hard copy.

16.8 All tenders shall be submitted without any deviations, alteration (or) modification, together with requisite Tender Security/EMD.

16.9 Telex, Facsimile or Emailed Tenders will be rejected.

16.10 Offer / Tender / Bid shall be as per the "Instructions to Tenderers", "General Conditions of Contract" and "Special Conditions of Contract" given in the Tender documents.

16.11 The Tenderer should avoid ambiguity in his Offer / Tender / Bid.

17. Deadline for submission of the Tenders

17.1 Tenders must be submitted online through Karnataka Public Procurement Portal (eProcurement Portal) on or before the date and time specified in the eProcurement Portal and in time submission of tender is the responsibility of the Tenderer. Original Documents (Hard copy) as listed under ITT clause 9.2 shall be submitted in the place, date & time as specified in ITT clause 16.7.

17.2 The Employer may, at their discretion, extend the deadline for submission of Tenders by issuing an amendment in accordance with ITT Clause 7, in which case all rights and obligations of the Employer and the Tenderers previously subject to the original deadline will thereafter be subjected to the deadline as extended.

18. Late Tenders

18.1 In online e-Procurement Portal, the Tenderer shall not be able to submit the Tender after the last date and time for submission as the icon for the task in the e-Procurement Portal will be disabled. Hardcopies received by BMRCL after the deadline for submission as mentioned in ITT clause 16.7 will be rejected.
Hard copies of those tenders which have been uploaded in the eProcurement portal successfully will only be considered for evaluation.

19. Modification and Withdrawal of Tenders

19.1 Tenderer may notify and correct or upload any relevant document in the portal till Tender submission date and time as published in the e-Procurement Portal.

19.2 No Tender shall be modified subsequent to the deadline for submission of Tenders.

19.3 Withdrawal or modification of a Tender between the deadline for submission of Tenders and the expiration of the original period of Tender validity specified in ITT Sub-clause 13.1 above or as extended pursuant to ITT Sub-clause 13.2 may result in the forfeiture of the Earnest Money Deposit pursuant to ITT Clause 14.

E. TENDER OPENING AND EVALUATION

20. Tender opening

20.1 **Qualification Cum Technical Package:**

20.1.1 **Opening of Qualification Cum Technical Package of all Tenderers:**

First, the Employer will open the EMD/Tender Security and verify the Tender Security/EMD at the date & time specified in the eProcurement Portal.

Further, the Employer will open the 'Qualification Cum Technical Package' of the Tenders whose EMD has been found acceptable, through e-Procurement Portal. If Tender Security/EMDs are not in proper form, the 'Qualification Cum Technical Package' will not be opened for such Tenderers.

Interested tenderers (or) their authorized representatives who choose to attend or may view the same on the portal on the scheduled date and time from their end. In the event of the specified date for Tender opening being declared a holiday by the Employer, the Tenders will be opened at the appointed time and location on the next working day.

20.1.2 The Tenderers will be examined for the following submittals:

i) Presence of valid Tender Security/EMD
ii) Presence of 'Qualification cum Technical Package' and all enclosures as per ITT clause 9.1 and,
iii) Submission of original documents as per ITT clause 9.2.

20.1.3 The Employer will evaluate and determine whether each Tender

(a) meets the eligibility criteria defined in ITT Clause 2;
(b) is accompanied by the required Earnest Money Deposit as per stipulations in ITT Clause 14; and
(c) meets the minimum qualification criteria stipulated in ITT Clause 3.

The Employer will draw out a list of qualified Tenderers.

20.1.4 Tenders which are not accompanied by a valid EMD / Tender Security, or are accompanied by an unacceptable or fraudulent EMD / Tender Security shall be considered as non-compliant and rejected. All decisions whether a Tender is non-responsive, unacceptable or whether a EMD / Tender Security is fraudulent or unacceptable or non-compliant will be that of the Employer.

20.1.5 If any Tender contains any deviation from the Tender documents and /or if the same does not contain Tender Security in the manner prescribed in the Tender documents, then that Tender is liable for rejection. Incomplete Tenders in respect of above would be rejected.

Tenderers, whose 'Qualification cum Technical Package' are found acceptable after evaluation, would be informed of the date and time of opening of 'Financial Package' through e-Procurement Portal.

20.2 **Financial Package**

20.2.1 Opening of Financial Package of Qualified Tenderers:

The Financial Package of the tenderers, whose 'Qualification cum Technical package' were found acceptable, will be opened in the presence of those Tenderers of their representatives, who choose to be present and also can view the opening on e-Procurement portal from their end. In the event of the specified date for Financial Package opening being declared a holiday by the Employer, the Tenders will be opened at the appointed time on the next working day.

20.2.2 The Tenderers' names, the Tender prices, the total amount of each Tender, and such other details as the Employer may consider appropriate, will be announced by the Employer at the opening. No Tender shall be rejected at Tender opening.

20.2.3 Further, it is to be noted that mere announcement of the tender prices, total amount quoted by the Tenderers shall not be construed as final, until and unless, the Employer determines the successful Tenderer taking into account ITT clauses 22, 23, 24, 25 & 34.

20.2.4 Conditional Tenders are not acceptable and will be summarily rejected.

20.2.5 The Employer shall prepare minutes of the Financial Package opening, including the information disclosed to those present in accordance with ITT Sub-clause 20.2.3.

21. Process to be confidential

21.1 Information relating to the examination, clarification, evaluation, and comparison of Tenders and recommendations for the award of a Contract shall not be disclosed to Tenderers or any other persons not officially concerned with such process until the award to the successful Tenderer has been announced.

21.2 From the time of Tender opening to the time of Contract award, no Tenderer shall contact the Employer on any matter related to the Tender, except on request and prior written permission.

21.3 Any effort by a Tenderer to influence the Employer's processing of Tenders or award decisions may result in the rejection of his Tender.

22. Clarification of Tender submittals

22.1 To assist in the examination, evaluation, and comparison of Tenders, the Employer may, at his discretion, ask any Tenderer for clarification of his Tender, including breakdowns of unit rates. The request for clarification and the response shall be in writing or by cable, but no change in the price or substance of the Tender shall be sought, offered, or permitted except as required to confirm the correction of arithmetic errors discovered by the Employer in the evaluation of the Tenders in accordance with ITT Sub-clause 24.

22.2 Subject to ITT Sub-clause 22.1, no Tenderer shall contact the Employer on any matter relating to its Tender from the time of the Tender opening to the time the Contract is awarded. If the Tenderer wishes to bring additional information to the notice of the Employer, it should do so in writing.

22.3 Any effort by the Tenderer to influence the Employer in the Employer’s Tender evaluation, Tender comparison or Contract award decisions may result in the rejection of the Tenderers’ Tender.

23. Examination of Tenders and determination of responsiveness

23.1 The Employer will examine the Tenders to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the Tenders are generally in order.

The Employer may waive any minor informality or non-conformity or irregularity in a Tender which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Tenderer.

23.2 A substantially responsive Tender is one which conforms to all the terms, conditions, and specifications of the Tender documents, without material deviation or reservation. A material deviation or reservation is one (a) which affects in any substantial way the scope, quality, or performance of the Works; (b) which limits in any substantial way, inconsistent with the Tender documents, the Employer's rights or the Tenderer's obligations under the Contract; or (c) whose

rectification would affect unfairly the competitive position of other Tenderers presenting substantially responsive Tenders.

23.3 If a Tender is not substantially responsive, it will be rejected by the Employer, and may not subsequently be made responsive by correction or withdrawal of the nonconforming deviation or reservation.

24. Correction of errors

24.1 The Item rates indicated in the Financial Package shall be final and no arithmetic corrections to the Tender prices shall be made. The Employer will evaluate and compare the Financial Packages of all Tenders as stipulated under ITT clause 25.

25. Evaluation and comparison of Tenders

25.1 The Employer will evaluate and compare only the Tenders determined to be substantially responsive in accordance with ITT Clause 23. No Tender will be considered if complete requirements covered in the schedule is not included in the Tender.

25.2 In evaluating the Tenders, the Employer will determine for each Tender the evaluated Tender Price by adjusting the Tender Price as follows:

(a) making any correction for errors pursuant to ITT Sub-clause 24; and

(b) making appropriate adjustments to reflect discounts or other price modifications offered.

25.3 The Employer reserves the right to accept or reject any variation, deviation or alternative offer. Variations, deviations and alternative offers, and other factors which are in excess of the requirements of the Tender documents or otherwise result in unsolicited benefits for the Employer shall not be taken into account in Tender evaluation.

25.4 The Tenders received will be evaluated by the Employer to ascertain the lowest acceptable Tender in the interest of the Employer, as specified in the specification and Tender documents. Evaluation criteria not mentioned herein but mentioned specifically in the technical specifications will be taken into consideration in the evaluation of offers.

25.5 The estimated effect of the price adjustment conditions, under relevant Clause of the General Conditions of Contract, during the implementation of the Contract, will not be taken into account in Tender Evaluation.

25.6 If the Tender of the successful Tenderer is seriously unbalanced in relation to the Employer's estimate of the cost of the work to be performed under the Contract, the Employer may require the Tenderer to produce detailed price analysis for any or all items of the Bill of Quantities, to demonstrate the internal consistency of those prices with the construction methods and schedule proposed. After evaluation of the price analysis, the Employer may require that the amount of the Performance Security set forth in ITT Clause 30 be increased at the expense of the successful Tenderer to a level sufficient to protect the Employer against financial loss in the event of default of the successful Tenderer under the Contract, subject to condition as specified in Special Conditions of Contract.

25.7 Bidders will be intimated to conduct mandatory POC (Proof of Concept) of the solution proposed, this will be considered for Technical evaluation.

F. AWARD OF CONTRACT

26. Award criteria

26.1 Subject to ITT Clause 28 and 34, the Employer will award the Contract to the Tenderer whose Tender has been determined to be substantially responsive to the Tender documents and who has offered the lowest evaluated Tender Price, provided that such Tenderer has been determined to be:

(a) eligible in accordance with the provisions of ITT Clause 2, and

(b) Qualified in accordance with the provisions of ITT Clause 3.

27. Employer's right to vary Quantities during the Contract

27.1 The Employer reserves the right during the pendency of Contract to increase or decrease the quantity of the items originally specified in the Bill of Quantity without any change in unit price or other terms and conditions as defined GCC Clause 34 and the Special Conditions of Contract.

28. Employer's right to accept any Tender and to reject any or all Tenders

28.1 Notwithstanding Clause 26, the Employer reserves the right to accept or reject any Tender, and to cancel the Tender process and reject all Tenders, at any time prior to the award of Contract, without thereby incurring any liability to the affected Tenderer/s or any obligation to inform the affected Tenderer/s of the grounds for the Employer's action. In such a case, EMD shall be released/returned promptly.

28.2 BMRCL reserves the right to accept the Tender in part or full which is beneficial to BMRCL. BMRCL's decision in this regard shall be final and binding.

29. Notification of award and signing of Agreement

29.1 The Tenderer whose Tender has been accepted will be notified of the award by the Employer prior to expiration of the Tender validity period by cable, email, telex or facsimile confirmed by registered letter. This letter (hereinafter and in the General Conditions of Contract called the "Letter of Acceptance") will state the sum that the Employer will pay the Contractor in consideration of the execution, completion, and maintenance of the Works by the Contractor as prescribed by the Contract (hereinafter and in the Contract called the "Contract Price").

29.2 Unless until a formal agreement is prepared and executed, the tender together with a "Letter of Acceptance" shall constitute a binding contract between both the parties.

29.3 The Agreement will incorporate all agreements between the Employer and the successful Tenderer within 30 days of receipt of LOA, the successful Tenderer will sign the Agreement and deliver it to the Employer.

29.4 Upon the furnishing of the Security Deposit by the Successful Tenderer, the Employer will promptly notify the other Tenderers that their Tenders have been unsuccessful and will discharge the Earnest Money Deposit, pursuant to ITT Clause 14.

29.5 The costs of stamp duties and similar charges imposed by law shall be borne by the Contractor.

30. Security deposit / Performance Security

30.1 Within 20 days of receipt of the Letter of Acceptance, the successful Tenderer shall deliver to the Employer, a Security deposit in accordance with GCC Clause 25 and format given in **Proforma-B of Section-9** for an amount as specified in 'Appendix to Form of Tender' (Section 4).

30.2 Failure of the successful Tenderer to comply with the requirements of ITT Sub-clause 30.1 shall constitute sufficient grounds for cancellation of the award and forfeiture of the Earnest Money Deposit.

31. Corrupt or Fraudulent practices

31.1 The BMRCL requires that the Tenderers observe the highest standard of ethics during the procurement and execution of such Government Financed Contracts. In pursuance of this policy, BMRCL:

(a) defines, for the purposes of this provision, the terms set forth as follows:

(i) "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in Contract execution; and

(ii) "Fraudulent practice" means any omission or misrepresentation of facts in order to influence a procurement process or the execution of a Contract to the detriment of BMRCL/Government, and includes collusive practice among Tenderers (prior to or after Tender submission) designed to establish Tender prices at artificial non-competitive levels and to deprive BMRCL of the benefits of free and open competition;

(b) will reject a proposal for award if it determines that the Tenderer recommended for award has engaged in corrupt or fraudulent practices in competing for the Contract in question;

(c) will declare a Tenderer (each member in case of JV/Consortium) ineligible, either indefinitely or for a stated period of time, to be awarded a Government financed Contract, if it at any time determines that the Tenderer has engaged in corrupt or fraudulent practices in competing for, or in executing, a Government financed Contract.

31.2 Furthermore, Tenderers shall be aware of the provision stated in Sub-clause 47.2 of the General Conditions of Contract.

32. One Tender per Tenderer

Each Tenderer shall submit only one Tender, either individually or as a member of a JV/ Consortium. A Tenderer who submits or participates in more than one Tender, either individually or as a member of a JV/Consortium, will cause all of the proposals with the Tenderer's participation to be disqualified. No Tenderer can be a Subcontractor while submitting a Tender individually or as a member of a JV/Consortium in the same Tender process. A Tenderer, if acting in the capacity of Subcontractor in any Tender, may participate in more than one Tender, but only in that capacity.

33. Site Visit

Not used.

G. PREFERENCE TO MAKE IN INDIA

34. Local Content & Purchase Preference

34.1 **Local Content (LC):**

Minimum "Local Content" (LC) shall be 50% for 'Class-I Local Tenderer' and 20% for 'Class-II Local Tenderer'.

All Tenderers shall certify in their Tender that the Local Content in their Tender. The Tenderer who certify in their Tender that LC is equal to or more than 50% shall be treated as 'Class-I Local Tenderer' and Local Content in their Tender is less than 50% and above 20% will be treated as Class-II Local Tenderer and Tenderer having Minimum Local Content less than 20% shall be treated as 'Non-Local Tenderer'.

Definitions of 'Class-I Local Tenderer', Class-II Local Tenderer' and 'Non-Local Tenderer' are is as mentioned in 'General Conditions of Contract' of this Tender document.

However, a Tenderer who has been debarred by any procuring entity, for violation of any Procurement Preference Order/Policy, shall not be eligible to participate in this bid process during the period of the debarment.

34.2 **Verification of 'Local Content' (LC):**

The Tenderer shall submit Self-certification, as per proforma given in 'Annexure-6', that the item/s offered meets the minimum 'local content' and shall give details of the locations(s) at which the local value addition is made as per Table-A & B of 'Attachment to Annexure-6'.

Imported items sourced locally from resellers/distributors are excluded from calculation of local content. Tenderer, shall submit along with tender, the details of imported items sourced locally from resellers/distributors as per Table C of 'Attachment to Annexure-6''.

Tenderers cannot claim themselves as Class-I local Tenderer/Class-II local Tenderer by claiming the services such as Transportation, Insurance, Installation, Testing & Commissioning, Training and after sales services support like DLP/AMC/CAMC etc., as local value addition as per DPIIT letter No. P-45021/102/2019-BE-II-Part (1) (E-50310) dated 04.03.2021

Absence of such certificates in their Tender submittals shall be treated as 'Non-local Tenderer' and shall be disqualified.

34.3 a) Tenderers shall note that the declaration regarding Local Content and its correctness shall be the sole responsibility of the Tenderer/Contractor. False declarations will be in breach of the Code of Integrity under Rule 175(1)(i)(h) of the General Financial Rules for which a Tenderer or its successors can be debarred for up to two (2) years as per Rule 151 (iii) of the General Financial Rules along with such other actions as may be permissible under law.

b) Tenderers are advised to note the contents of Government of India Order No. P-45021/2/2017-PP (BE-II)-Part (4) Vol.II dated 19.07.2024, issued by the 'Department for Promotion of Industry and Internal Trade' under the Ministry of Commerce and Industry regarding Public Procurement (Preference to make in India), with all its latest amendments as on the date of 'Notice Inviting Tender' for further clarification.

c) Tenderers are advised to note that the 'Local Content' is provided in this Tender as per the orders issued by respective Nodal Ministries as per Clause 14 of PP(PMI) Order dated 19.07.2024, Ministry of Housing and Urban Affairs letter No K-14011/08/2017/MRTS-Coord Dated 14.10.2020, Ministry of Electronics and Information Technology (MeitY) Electronic Products Notification No. W-43/4/2019-IPHW-MeitY dated 07.09.2020 and Gazette Notification dated 06.03.2024.

d) Tenderers are also advised to note the contents of Government of India Office Memorandum No. P-45021/102/2019-BE-II-Part (1) (E-50310) dated 04.03.2021 issued by the 'Department of Promotion of Industry and Internal Trade' under the Ministry of Commerce and Industry, regarding clarification on local content.

e) In case DPIIT's Order no. P-45021/2/2017-PP(BE-II) dated 16.09.2020 is referred in this tender document, the same is superseded by this Order No. P-45021/2/2017-PP (BE-II)-Part(4) Vol.II dated 19.07.2024.

34.4 **Purchase Preference**

'Class-I Local Tenderer' shall be eligible for availing Purchase Preference over 'Class-II Local Tenderer' and the Margin of Purchase Preference (MOPP) of 20% shall be given to the "Class-I Local Tenderer"'.

'Class-II Local Tenderer' will not get purchase preference.

However, a Tenderer who has been debarred by any procuring entity, for violation of any Procurement Preference Order/Policy, shall not be eligible for purchase preference for the duration of debarment.

34.4.1 Non-divisible Tendered Work

The Tendered work is not divisible in nature, hence, in terms of clauses 3A(c) and 3A(d) of Public Procurement (Preference to Make in India) Order 2017- Revision dated 19.07.2024, the Contract for the Tendered works shall be awarded as below:

(i) Among all qualified Tenderers, the lowest evaluated Tenderer will be termed as L1. If L1 is from a 'Class-I Local Tenderer', the Contract for the full quantity will be awarded to L1.

(ii) If L1 is not 'Class-I Local Tenderer', the lowest bidder among the 'Class-I Local Tenderer', will be invited to match the L1 price subject to Class-I Local Tenderer's quoted price falling within the margin of purchase preference, and the Contract for the full quantity shall be awarded to such 'Class-I Local Tenderer' subject to matching the L1 price.

(iii) In case such lowest eligible 'Class-I Local Tenderer' fails to match the L1 price, the 'Class-I Local Tenderer' with the next higher bid within the margin of purchase preference shall be invited to match the L1 price and so on and contract shall be awarded for the full quantity accordingly. In case none of the 'Class-I Local Tenderer' within the margin of purchase preference matches the L1 price, the contract may be awarded to the L1 bidder for the full quantity.

(iv) 'Class-II Local Tenderer' will not get purchase preference in this Tender.

34.4.2 Determination of Contract prices of 'Class-I Local Tenderer' under Purchase Preference:

(a) In the event of Lowest 'Class-I Local Tenderer' agreeing in writing to match the 'Tender Total' of the lowest evaluated Tenderer (L1), in accordance with ITT Clause 34.4.1, the 'Evaluated Tender Total' of 'Class-I Local Tenderer' shall be adjusted to match with the 'Evaluated Tender Total' of the lowest evaluated Tenderer (L1).

(b) Tenderers shall note that the adjustment of price/s under purchase preference shall generally be made as above. However, in any peculiar cases, which do not get covered as per the above stated procedure, the Employer at his discretion shall adopt an appropriate methodology which is beneficial/ advantageous to the Employer for adjustment of prices. The Employer's decision in this regard shall be final and binding on the Tenderer.

(c) Notwithstanding, it shall be ensured that after adjustment, the Tender Total of the Class-I Local Tenderer shall be equal to the Tender Total of lowest evaluated price (L1).

35. Eligible Source Countries of the Tenderer

35.1 Any Tenderer, from a country which shares a land border with India, to which the Govt. of India has not extended lines of credit or in which the Govt. of India is not engaged in development projects, will be eligible to bid in this tender only if the Tenderer is registered with the "Competent Authority".

Further, any Tenderer (including Tenderer from India) having specified 'Transfer of Technology' (ToT) arrangement with an entity from a country which shares a land border with India, shall also require to be registered with the same Competent Authority.

['Competent Authority' shall be as defined in Annexure-I of Order (Public Procurement No. 4) issued by Procurement Policy Division, Department of Expenditure, Ministry of Finance, Govt. of India vide No. F.7/10/2021-PPD(1) dated 23.02.2023]. Tenderers are advised to note and comply with the contents of the said order/s.

35.2 The successful Tenderer shall not be allowed to subcontract works to any Contractor from a country, which shares a land border with India, to which the Govt. of India has not extended lines of credit or in which the Govt. of India is not engaged in development projects, unless such Contractor is registered with the “Competent Authority”.

35.3 In this regard, the Tenderer shall provide a certificate as per Proforma given in ‘Annexure-7’. If such certificate given by the Tenderer whose bid is accepted is found to be false, this would be a ground for immediate termination and further legal action in accordance with law.

--- xxx ---

PAGE INTENTIONALLY LEFT BLANK

SECTION 3: QUALIFICATION INFORMATION

1. The information to be filled in by the Tenderer hereunder will be used for purposes of evaluating the eligibility and qualification of the Tenderer as provided for in Clause 3 of the Instructions to Tenderers. This information will not be incorporated in the Contract.

1.1	Constitution or legal status of Tenderer	[Attach copy]
	Agency in which Registered (with Registration No.)	…… (Attach Copy)
	Principal place of business:	……

		Financial Year	Total Value of works for the year	Multiplication factor for updation of Value of Work to FY 2024-25	Total value of Works updated to FY 2024-25
1.2	Total value of works* executed and payments received year wise in the last five years (in Rs. Lakhs) #	FY 2019-20		1.40	
		FY 2020-21		1.31	
		FY 2021-22		1.22	
		FY 2022-23		1.14	
		FY 2023-24		1.07	

***** Value of work as defined in ITT clause 3

- Attach Certificate from practicing Chartered Accountant

1.3 Information on works which are yet to be completed and works for which Tenders have been submitted as on the date of this Tender.

(A) Existing commitments and on-going works:

Description of Work	Place & State	Contract No. & Date	Name and Address of Employer	Value of Contract (Rs. Lakh)	Stipulated period of completion	Value of works remaining to be completed (Rs. Lakh)	Anticipated date of completion
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

……..
……..

(B) Works for which Tenders already submitted:

Description of Work	Place & State	Name and Address of Employer	Estimated value of works (Rs. Lakh)	Stipulated period of completion	Date when decision is expected	Remarks if any
(1)	(2)	(3)	(4)	(5)	(6)	(7)

……..
……..

1.4 Work performed as Prime Contractor (in the same name) on works of similar nature during the last five years counted 28 days prior to the date of Tender submission *[with respect to ITT clause 3.3]*.

Project Name	Name of Employer	Description of Work	Contract Number	Value of contract Rs. Lakhs	Date of issue of Work order	Specified period of completion	Actual date of completion	Remarks explaining reasons for delay in completion of work
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)

……..
……..

1.5 Reports on the audited statements of financial standing of the Tenderer, such as profit and loss statements, balance sheet and Auditor's reports for the last five years (Provisional Financial statements are not acceptable);

1.6 Qualification and experience of the key technical and Management personnel in permanent employment with the Tenderer and those that are proposed to be deployed on this Contract, if awarded.

1.7 Not Used.

1.8 Evidence of access to financial resources to meet the qualification requirement specified in ITT Clause 3.3.2: Cash in hand, Letter of Credit, etc. List them below and attach certificate from the Banker in the suggested format as under:

BANKER'S CERTIFICATE

This is to certify that M/s. …….. is a reputed company with a good financial standing. If the Contract for this work, namely "…… *(name of the work)* ……" is awarded to the above firm, we shall be able to provide overdraft / credit facilities to the extent of Rs. …… to meet the working capital requirements for executing the above Contract.

Sd/-
Name of the Bank, Senior Bank Manger
Address: ……..

FINANCIAL RESOURCES
(For Liquidity)

1. Specify proposed sources of financing to meet the requirement of liquidity in the form of lines of credit (Banker's Certificate) sufficient for total cash flow demands of the subject works specified.

Financial Resources		
No.	Source of financing from different Banks	Amount (INR equivalent)
1		
2		
3		
4		
5		

2. The tenderer shall provide original banker's Certificate issued not earlier than 06 months from the date of submission of Tender as per format provided above.

1.9 Information on litigations in which the Tenderer is involved.

Employer	Other Party(ies)	Details of dispute	Amount involved	Remarks showing present status

……..
……..

--- xxx ---

PAGE INTENTIONALLY LEFT BLANK

SECTION 4: FORM OF TENDER

NIT No : ……..

Description of Work: …….

To:
…….,
…….*(name and complete address of the employer)*,
……..,
Bengaluru, PIN: ……..,
Karnataka, India.

Dear Sir / Madam,

1 Having examined and understood the Instructions to Tenderer, General Conditions of the Contract, Special Conditions of Contract, Technical Specifications and any other documents forming part of the Tender document issued under Tender notification no _____ dated _____ including any addendum /amendments, the receipt of which is hereby duly acknowledged, I/We the undersigned, hereby submit the fully completed Tender documents online through Karnataka Public Procurement Portal, which includes the following for the said work;

   a) Tender Security / Earnest Money Deposit (EMD)
   b) Qualification cum Technical Package
   c) Financial Package.

2 I/We hereby agree to submit the original documents in hardcopy as stipulated under ITT clause 19.2.

3 I/We hereby agree to execute the Contract in conformity with the Specifications & Conditions of Contract enumerated in the Tender Documents, for the sum stated & quoted in the Tender or such other sums as may be ascertained in accordance with the 'Bill of Quantities' which are made part of the Financial Package.

4 This Tender and your written acceptance of it shall constitute a binding Contract between us. We understand that you are not bound to accept the lowest or any Tender you receive.

5 We undertake that, in competing for (and, if the award is made to us, in executing) the above Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

6 We hereby confirm that this Tender complies with the Tender validity and Earnest Money Deposit required by the Tender documents.

7 We undertake, if our Tender is accepted, to execute the Works in accordance with the Stipulated Completion Date specified in the 'Appendix to Form of Tender'.

8 If our Tender is accepted, we will submit the Performance Security for a sum equivalent to Ten (10) percent of the Contract Price for the due performance of the Contract, in the form as prescribed in the Clause 25 of GCC.

9 We agree to abide by this Tender for the Tender validity period specified in ITT Clause 13 and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

10 We confirm that we comply with the eligibility requirements as per ITT Clause 2 and clause 3 of the Tender documents.

11 We have read and understood the requirement of Local Content in accordance to ITT clause 34 & 'Margin of Purchase Preference' in accordance to ITT clause 34.4 and Eligible sources countries of the Tenderer in accordance to ITT clause 35.

Dated this ..... day of ..... 20.....

Yours faithfully,

_____
(Signature) (in the capacity of)

Duly authorized to sign Tender for and on behalf of
"……"

(To be digitally signed, using Digital Signature Certificate (Only Class III Certificates with signing + encryption key usage issued by any Certifying Authority recognized by CCA India), by the authorised signatory of the Tenderer on Tenderer's letter pad).

APPENDIX TO FORM OF TENDER

SALIENT FEATURES OF CONTRACTS (CONTRACT DATA)

Sl.No.	Item	Particulars
1.	Employer's Name & Address	Bangalore Metro Rail Corporation Limited 3rd Floor, BMTC Complex (C-Block) K H Road, Shanthinagar Bangalore, PIN: 560027 Karnataka, India
2.	Warranty / Defects Liability Period (GCC clause 50)	The Warranty/Defects Liability Period shall start from the date of acceptance by the Employer and shall continue until **12 months** from that date of 'Go-live'.
3.	Validity of Tender (ITT clause 13)	**120 days** from the latest date of submission of Tenders as per ITT clause 13.
4.	Tender Security / Earnest Money Deposit (EMD) (See Clause 14 of ITT)	Earnest Money Deposit (EMD) of **INR 6,99,200 (Indian Rupees Six Lakh Ninety-nine Thousand Two Hundred only)** as defined in ITT Clause 14. In case the EMD is submitted in the form of BG/eBG, such BG/eBG shall be valid for 45 days beyond the validity of the Tender (i.e. 120+45 = **165 days** from the latest date of submission of Tender).
5.	Contractor's Name & Address with telephone No and e-mail id	*……(To be filled in by the Tenderer) ……*
6.	Submission of queries and pre-bid meeting, date and time of Tender Submission, Tender opening and Place.	• **Last date for submission of queries by Tenderers:** As specified in eProcurement Portal • **Date of Pre-bid meeting:** As specified in eProcurement Portal • **Date for Tender Submission:** As specified in eProcurement Portal • **Date for Tender Opening:** As specified in eProcurement Portal • **Place:** Office of the Managing Director Bangalore Metro Rail Corporation Limited 3rd Floor, BMTC Complex (C-Block) K H Road, Shanthinagar, Bangalore – 560027, Karnataka, India.
7.	The Work consists of	Establishment, integration and Commissioning of On-premises "Security Operation Center" (SOC) for IT & CCTV Network of Bangalore Metro Rail Project and Operation & Maintenance of SOC for 3 years after Go Live Management of On-premises SOC on 24x7 basis throughout the year at Baiyappanahalli, BMRCL.
8.	Start Date (Date of commencement of works)	The date of issue of 'Letter of Acceptance' (LOA).

9.	The Stipulated Completion Date for the whole of the Works	**42 months** from the start date (i.e. 6 months for completion of works from the start date; CAMC for 2 years after warranty/DLP of 1 year from Go-live, and Operation of SOC for 3 years from Go-live).
10.	The following documents also form part of the Contract (See Clause 2.2 of GCC)	(1) Contract Agreement (2) Letter of Acceptance, Notice to Proceed with the works (3) Instruction to Tenderers/ Bidders (4) General Conditions of Contract (5) Special Conditions of Contract (6) Form of Tender / Bid Form (7) Technical Specifications including scope of work (8) Bill of quantities (9) Contractor's Proposals (10) All correspondence between the Tenderer and BMRCL from the date of issue of NIT and the date of issue of the LOA. (11) Any other document forming part of the Contract.
11.	Amount of **Performance Security** (See Clause 25 of GCC)	**10% of the Contract Value in INR.** In the event of variations during the execution of the Contract which result in payments to the Contractor over and above the original Contract Price, the Performance Security shall be suitably adjusted at every 6 months at the request of the Employer. The Performance Security shall be in the form of **Demand Draft / Pay Order / Banker's Cheque / Electronic Bank Guarantee** or **Bank Guarantee** drawn on and **payable & extendable at a designated branch in Bengaluru.**
12.	Liquidated Damages (See Clause 40 of GCC)	The liquidated damages for the whole of the works are Rs. 46,600 *(usually 0.1% of the Contract Price)* per day. The maximum amount of liquidated damages for the whole of the works is **ten percent (10%)** of final Contract Price.
13.	Program & Methodology (see clause 21 of GCC)	Work Program & Methodology shall be submitted within 15 days of issue of LOA or earlier as required by the Employer/Engineer.
14.	Payment upon Termination – **Computation of additional cost to the Employer** (GCC Clause 47.1)	The percentage to apply to the value of the work not completed representing the Employer's additional cost for completing the Works shall be **30 percent**.

15.	**Insurance** (GCC clause 26)	

Sl.No	**Type of Cover**	**Minimum cover for Insurance[1]**
(i)	Works and of Plant and materials	The Sum stated in the Agreement plus 20%
(ii)	Loss or damage to equipment	Full replacement cost
(iii)	Loss or damage to property	Full replacement cost
(iv)	Personal injury or death Insurance (a) For Third Party[2]	10% of the Contract Amount.
	(b) For Contractor's Employees or labour.	In accordance with the statutory requirements applicable to Karnataka.

[1] *Employer to specify as per requirement. Exclusions if any should also be specified*

[2] *Specify an appropriate figure as per the latest Govt. Order or guidelines or statutory requirements.*

PAGE INTENTIONALLY LEFT BLANK

SECTION 5 : GENERAL CONDITIONS OF CONTRACT

Contents

A. GENERAL **37**

1. DEFINITIONS 37
2. INTERPRETATION 39
3. LAW GOVERNING CONTRACT 40
4. EMPLOYER'S DECISIONS 40
5. DELEGATION 40
6. COMMUNICATIONS 40
7. NOT USED 40
8. OTHER CONTRACTORS 40
9. PERSONNEL 40
10. EMPLOYER'S AND CONTRACTOR'S RISKS 41
11. EMPLOYER'S RISKS 41
12. CONTRACTOR'S RISKS 41
13. NOT USED 41
14. CONTRACTOR TO EXECUTE THE WORKS 41
15. THE WORKS TO BE COMPLETED BY THE STIPULATED COMPLETION DATE 41
16. SAFETY 41
17. NOT USED 41
18. POSSESSION OF THE SITE 41
19. ACCESS TO THE SITE 42
20. INSTRUCTIONS 42

B. TIME CONTROL **42**

21. PROGRAM 42
22. EXTENSION OF THE STIPULATED COMPLETION DATE 42
23. DELAY ORDERED BY THE EMPLOYER 42
24. MANAGEMENT MEETINGS 42
25. PERFORMANCE SECURITY / SECURITY DEPOSIT 42
26. INSURANCE 44

C. QUALITY CONTROL **44**

27. IDENTIFYING DEFECTS 44
28. TESTS 45
29. CORRECTION OF DEFECTS 45
30. UNCORRECTED DEFECTS 45
31. INSPECTIONS AND TESTS 45
32. ACCEPTANCE CERTIFICATES 45

D. COST CONTROL **46**

33. BILL OF QUANTITIES (BOQ) 46
34. VARIATIONS 46
35. PAYMENTS FOR VARIATIONS 46
36. SUBMISSION OF BILLS FOR PAYMENT 46
37. PAYMENTS 47
38. NOT USED 47
39. TAXES & DUTIES 47
40. LIQUIDATED DAMAGES 47
41. COST OF REPAIRS 47

E. FINISHING THE CONTRACT **47**

42. COMPLETION 47
43. TAKING OVER 47
44. FINAL BILL / ACCOUNT 47
45. "OPERATING AND MAINTENANCE MANUALS" 48
46. TERMINATION 48
47. PAYMENT UPON TERMINATION 49
48. PROPERTY 49
49. RELEASE FROM PERFORMANCE 49

F. OTHERS **49**

50. WARRANTY / DEFECTS LIABILITY PERIOD 49
51. FORCE MAJEURE 50
52. Claims, Disputes and Conciliation 50
53. PATENT RIGHTS 53
54. LIMITATION OF LIABILITY 53
55. GOVERNING LANGUAGE 53
56. THE COURTS OF JURISDICTION 53
57. NOTICES 53
58. USE OF CONTRACT DOCUMENTS AND INFORMATION; INSPECTION AND AUDIT BY THE GOVERNMENT 54

SECTION - 5

GENERAL CONDITIONS OF CONTRACT

A. General

1. Definitions

1.1 Terms which are defined in the 'Appendix to Form of Tender' are not also defined in the General Conditions of Contract but keep their defined meanings. Bold letters are used to identify defined terms.

a. **"Bill of Quantities"** means the priced and completed Bill of Quantities forming part of the Tender.

b. The **"Completion Date"** is the date of completion of the whole of the Works certified by the Employer in accordance with Sub Clause 42.1 of GCC.

c. The **"Contract"** is the Contract between the Employer and the Contractor to execute, complete and maintain the Works. It consists of the documents listed in GCC Clause 2.2.

d. The **"Contractor"** is a person or corporate body whose Tender to carry out the Works has been accepted by the Employer. It means the person, firm or company with whom the order of the Works is placed and shall be deemed to include the Contractor's successors (approved by the Employer), representatives, heirs, executors and administrators, as the case may be unless excluded by the terms of the Contract.

e. The **"Contractor's Tender"** is the completed Tender document submitted by the Contractor to the Employer.

f. The **"Contract Value"** or **"Contract Price"** means the price payable to the Contractor under the Contract for the full and proper performance of its Contractual obligations.

g. **"Days"** are calendar days; **"months"** are calendar months.

h. A **"Defect"** is any part of the Works not completed in accordance with the Contract.

i. The **"Defects Liability Period"** is the period mentioned in the 'Appendix to Form of Tender' and calculated from the Completion Date in accordance with Clause 50 of GCC.

j. The **"Employer"** or **"BMRCL"** means the Bangalore Metro Rail Corporation Limited or the person named as such in the Tender document and includes the legal successors or permitted assigns of the Employer.

k. **"Engineer"** means any person/party nominated or appointed from time to time by the Employer to act as the Engineer for the purposes of the Contract and notified as such in writing to the Contractor.

l. **"Engineer's representative"** means any person nominated by Engineer with the approval of the Employer who shall exercise the authority of the Engineer to the extent notified by the Engineer.

m. **"Equipment"** is the Contractor's machinery and vehicles brought temporarily to the Site to construct/ execute the Works.

n. The **"Initial Contract price"** is the Contract Price listed in the Employer's Letter of Acceptance.

o. **"Letter of Acceptance"** means the letter or memorandum communicating to the Successful Tenderer the acceptance of his Tender and includes other communication modes included in the Instructions to Tenderers.

p. **"Materials"** are all supplies, including consumables, used by the Contractor for incorporation in the Works.

q. **"Notice to Proceed"** means the notice issued by the Employer to the Contractor to proceed with the works at the site.

r. **"Appendix to Form of Tender"** is the Salient Features of Contract that defines the documents and other information which comprise the Contract.

s. **"Signed"** includes stamped, except in the case of acceptance of Tender or any amendment thereof;

t. **"Specification"** means the Specification of the Works included in the Contract and any modification or addition made or approved by the Employer.

u. The **"Start Date"** shall be the date of issue of 'Letter of Acceptance' (LOA) or the date specified in the 'Notice to Proceed', as the case may be.

v. The **"Stipulated Completion Date"** is the date on which it is intended that the Contractor shall complete the Works. The Stipulated Completion Date is specified in the 'Appendix to Form of Tender'. The Stipulated Completion Date may be revised only by the Employer by issuing an extension of time.

w. A **"Subcontractor"** is a person or corporate body who has a Contract with the Contractor to carry out a part of the work in the Contract which includes work on the Site.

x. A **"Variation"** is an instruction given by the Employer which varies the Works.

y. **"Works"** means what the Contract requires the Contractor to construct, install, and turn over to the Employer, as defined in the Contract Data/Description of the work/Technical specifications/Scope of works.

z. "**Plant**" is any integral part of the Works which is to have a mechanical, electrical, electronic or chemical or biological function.

aa. "**Project Site**" or "**Site**" or "**SOC**' means the 'Security Operation Centre' specified in the Contract to be established by the Contractor under the Contract or any other place approved by the Employer for the purpose.

bb. '**Class-I Local Tenderer**' means a Tenderer or service provider, whose goods, services or works offered for procurement meets the minimum local content as prescribed for 'Class-I Local Tenderer' under ITT clause 34.

cc. **'Class-II Local Tenderer'** means a Tenderer or service provider, whose goods, services or works offered for procurement meets the minimum local content as prescribed for 'Class-II local Tenderer' but less than that prescribed for 'Class-I local Tenderer' under ITT clause 34.

dd. Non-local Tenderer' means a Tenderer or service provider, whose goods, services or works offered for procurement, has local content less than that prescribed for 'Class-II Local Tenderer' under ITT clause 34.

ee. '**Local Content**' means the amount of value added in India which shall, unless otherwise prescribed by the Nodal Ministry, be the total value of the item procured (excluding net domestic in direct taxes) minus the value of imported content in the item (including all customs duties) as a proportion of the total value, in percent.

Explanatory notes for calculation of local content given above:
(a) Imported items sourced locally from resellers/distributors shall be excluded from calculation of local content.

(b) The license fees/royalties paid/ technical charges paid out of India shall be excluded from local content calculation.

(c) Procurement/Supply of repackaged/refurbished/rebranded imported products as understood commonly shall be treated as reselling of imported products and shall be excluded from calculation of local content. The definition of repackaged/ refurbished/ rebranded imported products is as follows;

'Refurbishing' means repair or reconditioning of an imported product does not amount to manufacture because no new goods come into existence.

'Repackaging' means repacking of imported goods from bulk pack to smaller packs would not ordinarily amount to manufacture of a new item."

'Rebranding' means relabelling or renaming or change in symbol or logo/makes or corporate image of a company/organization/firm for an imported product would amount to rebranding.

(d) To ensure that imported items sourced locally from resellers/distributors are excluded from calculation of local content, procuring entities to obtain from bidders, the cost of such locally-sourced imported items (Inclusive of taxes) along with break-up on license/royalties paid/technical expertise cost etc. sourced from outside India. For items sold by bidder as reseller, OEM certificate for country of origin to be submitted.

(e) For contracts involving supply of multiple items, weighted average of all items to be taken while calculating the local content.

The percentage of Local content shall be exclusive of the Services such as transportation, insurance, installation, commissioning, training and after sales services support like DLP/AMC/CAMC etc., in line with OM No. P-45021/102/2019-BE-II-Part (1) (E-50310) dated 04.03.2021.

ff. **'L1'** means the lowest Tender received in this Tendering process as adjudged in the evaluation process as per the Tender.

gg. **'Nodal Ministry'** means the Ministry or Department identified pursuant to this Tender in respect of a particular item of goods or services or works.

hh. '**Procuring Entity**' means 'the Employer" or BMRCL, i.e. Bangalore Metro Rail Corporation Ltd.

2. Interpretation

2.1 In interpreting these General Conditions of Contract and Special Conditions of Contract, singular also means plural, male also means female or neuter, and the other way around. Headings have no significance. Words have their normal meaning under the language of the Contract unless

specifically defined. “Tender” / “Tendering” / “Tenderer” shall also mean “Bid” / “Bidding” / “Bidder”. "Offer" also mean Tender / Bid.

2.2 The documents forming the Contract shall be interpreted in the following order of priority:

(1) Contract Agreement
(2) Letter of Acceptance, notice to proceed with the works
(3) Bill of quantities
(4) Technical Specifications
(5) Special Conditions of Contract
(6) General Conditions of Contract

3. Law governing Contract

3.1 The law governing the Contract is the Laws of India supplanted by the Karnataka Local Acts.

4. Employer's decisions

4.1 Except where otherwise specifically stated, the Employer will decide contractual matters between the Employer and the Contractor.

5. Delegation

5.1 The Employer may delegate any of his duties and responsibilities to other people after notifying the Contractor and may cancel any delegation after notifying the Contractor.

6. Communications

6.1 Communications between parties which are referred to in the conditions are effective only when in writing. A notice shall be effective only when it is delivered (in terms of Indian Contract Act).

7. Not Used

8. Other Contractors

8.1 The Contractor shall cooperate and share the Site with other Contractors, public authorities, utilities, and the Employer.

9. Personnel

9.1 The Contractor shall, unless otherwise provided in the Contract, make his own arrangements for the engagement of all staff and labour, local or other, and for their payment, housing, feeding and transport.

9.2 The Contractor shall employ the technical personnel (of number and qualifications) as may be stipulated by BMRCL from time to time during the execution of the work. The technical staff so employed shall be available at site as may be stipulated by the Employer.

9.3 If the Employer asks the Contractor to remove a person who is a member of the Contractor’s staff or his work force stating the reasons, the Contractor shall ensure that the person leaves the Site within seven days and has no further connection with the work in the Contract.

9.4 **Compliance with Labour Regulations**

9.4.1. The Contractor shall, if required by the Employer, deliver to the Employer a return in detail, in such form and at such intervals as the Employer may prescribe, showing the staff and the numbers of the several classes of labour from time to time employed by the Contractor on the Site and such other information as the Employer may require.

10. Employer's and Contractor's risks

10.1 The Employer carries the risks which this Contract states are Employer's risks, and the Contractor carries the risks which this Contract states are Contractor's risks.

11. Employer's risks

11.1 The Employer is responsible for the excepted risks which are:

a) rebellion, riot commotion or disorder unless solely restricted to employees of the Contractor or his Subcontractors arising from the conduct of the Works; or
b) a cause due solely to the design of the Works, other than the Contractor's design; or
c) any operation of the forces of nature (in so far as it occurs on the Site) which an experienced Contractor:
   i) could not have reasonably foreseen; or
   ii) could reasonably have foreseen, but against which he could not reasonably have taken at least one of the following measures:
      1. prevent loss or damage to physical property from occurring by taking appropriate measures, or
      2. Insure against such loss or damage.

12. Contractor's risks

12.1 All risks of loss of or damage to physical property and of personal injury and death which arise during and in consequence of the performance of the Contract other than the excepted risks are the responsibility of the Contractor.

13. Not used

14. Contractor to execute the Works

14.1 The Contractor shall execute the Works in accordance with the Specification and drawings.

15. The Works to be completed by the Stipulated Completion Date

15.1 The Contractor may commence execution of the Works on the Start Date and shall carry out the Works in accordance with the program submitted by the Contractor, as updated with the approval of the Employer, and complete them by the Stipulated Completion Date.

16. Safety

16.1 The Contractor shall be responsible for the safety of all activities on the Site.

17. Not used

18. Possession of the Site

18.1 The Employer shall give possession of all parts of the Site to the Contractor. If possession of site or a part of site is not given by the date stated in the Contract or Notice to proceed, the reasonable

extension of time may be given. However, no monetary claims whatsoever shall be paid to the Contractor or entertained on this account.

19. Access to the Site

19.1 The Contractor shall allow the Employer and any person authorized by the Employer access to the SOC.

20. Instructions

20.1 The Contractor shall carry out all instructions of the Employer which comply with the applicable laws, where the Site is located.

B. Time Control

21. Program

21.1 Within the time stated in the 'Appendix to Form of Tender', the Contractor shall submit to the Employer for approval a Program showing the general methods, arrangements, order, and timing for all the activities in the Works within 15 days from the date of issue of LOA or earlier as required by the Employer.

21.2 The Employer's approval of the Program shall not alter the Contractor's obligations. The Contractor may revise the Program and submit it to the Employer again at any time. A revised Program is to show the effect of Variations.

22. Extension of the stipulated completion date

22.1 The Employer shall extend the stipulated completion date, if a Variation is issued and which makes it impossible for Completion to be achieved by the Stipulated Completion Date.

22.2 The Employer shall decide whether and by how much to extend the Stipulated Completion Date within 21 days of the Contractor asking the Employer for a decision upon the effect of a Variation and submitting full supporting information.

23. Delay ordered by the Employer

23.1 The Employer may instruct the Contractor to delay the start or progress of any activity within the Works. However, no monetary claims whatsoever shall be paid to the Contractor or entertained on this account.

24. Management meetings

24.1 The Employer may require the Contractor to attend a Management meeting. The business of a Management meeting shall be to review the progress achieved and the plans for remaining work.

24.2 The responsibility of the parties for actions to be taken is to be decided by the Employer either at the Management meeting or after the management meeting and stated in writing to be distributed to all who attended the meeting.

25. Performance Security / Security Deposit

25.1 Within 20 days of receipt of notification communicated by the Employer by issue of "Letter of Acceptance", the Contractor shall furnish a Performance Security (including additional security for unbalanced Tenders, if required) for an amount as specified in **Appendix to Form of Tender (Section 4)** in one of the following forms:

(a) A crossed **Demand Draft / Pay Order / Banker's Cheque** in favour of the "Bangalore Metro Rail Corporation Ltd," from an Indian Scheduled Bank (excluding Cooperative Banks) or from a Scheduled Foreign Bank as defined in Section 2(e) of RBI Act 1934 read with Second Schedule, **payable at Bengaluru**.

or

(b) An irrevocable **Electronic Bank Guarantee (eBG) or Bank Guarantee** issued from an Indian Scheduled Bank (excluding Cooperative Banks) or from a Scheduled Foreign Bank as defined in Section 2(e) of RBI Act 1934 read with Second Schedule drawn on and payable & extendable at a designated branch in Bengaluru in the Form given in Proforma-B of Section 9 to the Tender documents. However, 'Performance Security' Bank Guarantee format is also available in https://tenderb.bmrc.co.in.

In case furnishing of an acceptable Performance Security is delayed by the Contractor beyond the period provided in GCC clause 25.1, the Employer may forfeit the Earnest Money Deposit / Tender Security.

25.2 On the performance and completion of the Contract in all respects the Performance Security will be converted into Guarantee to warrant the Defect Liability obligations of the Contractor. The Performance Security shall be valid up to 3 months beyond the Defects Liability Period for the Entire Work and the additional security for unbalanced Tenders shall be valid until a date 30 days from the date of issue of the certificate of completion. The Performance Security will be returned within 3 months after satisfactory completion of Defects Liability Period.

25.3 The Employer shall be entitled and it shall be lawful on his part to forfeit the amount of the Performance Security in whole or in part in the event of any default, failure or neglect on the part of the Contractor in the fulfillment or performance in all respects of the Contract under reference or any other Contract with the Employer.

The Employer shall also be entitled to deduct from the amount of the Performance Security any loss or damage which the Employer may suffer or be put by reason of or due to any act or other default, recoverable by the Employer from the Contractor in respect of the Contract under reference or any other Contract.

On occurrence of either of the aforesaid events, the Employer shall call upon the Contractor to maintain the amount of the Performance Security as its original limit by furnishing fresh Bank Guarantee of additional amount, provided further that the Employer shall be entitled to recover any such claim from any sum then due or which at any time thereafter may become due to the Contractor under this or any other Contracts with the Employer.

25.4 The Performance Security shall remain in full force and effect during the period that would be taken for satisfactory performance/ completion of the Works and fulfillment in all respects of the Contract and shall in the first instance be valid until 3 months beyond Defects Liability Period. Before the expiry of the date of validity of the Performance Security, the Contractor on being called upon by the Employer from time to time shall obtain from the Guarantee Bank, extension of time for validity thereof for a period of six (6) months, on each occasion. The extension or extensions aforesaid, executed on non-judicial stamp paper of appropriate value must reach the Employer at least thirty days before the date of expiry of the Performance Security on each occasion.

25.5 As and when an amendment is issued to the Contract, the Contractor shall, within 15 days of the receipt of such an amendment furnish to the Employer an amendment to the Performance Security rendering the same valid for the Contract as amended and up to 3 months beyond amended completion of Defects Liability Period. All expenses of this shall be borne by the Contractor.

25.6 The Performance Security and or any amendment thereto shall be executed on a Non Judicial stamp paper of requisite money value in accordance with the laws of the country in which the same is/are executed by the party competent to do so.

25.7 If the Contractor, having been called upon by the Employer to furnish Performance Security, fails to furnish the same, it shall be lawful for the Employer:

i) to recover from the Contractor, the amount of Performance Security by deducting the amount from the pending bills of the Contractor under any Contract with the Employer or the Government or any other person contracting through the Employer or otherwise however, OR

ii) to cancel the Contract or any part thereof and to execute or authorize to execution of the Works at the risk and cost of the Contractor and in that event, the provisions of clause 46 & 47 shall apply as far as applicable.

26. Insurance

26.1 The Contractor shall prior to commencing the works, effect and thereafter maintain insurances, in the joint names of the Employer and the Contractor, (cover from the first working day after the Start Date to the end of Defects Liability Period), in the amounts stated in the 'Appendix to Form of Tender':

(a) for loss of or damage to the Works, Plants and Materials and the Contractor's equipment;

(b) for liability of both Parties for loss, damage, death and injury to third parties or their property arising out of the Contractor's performance of the Contract including the Contractor's liability for damage to the Employer's property other than the Works and

(c) for liability of both Parties and of any Employer's representative for death and injury to the Contractor's personnel except to the extent that liability arises from the negligence of the Employer, any Employer's representative or their Employees.

26.2 Policies and certificates for insurance shall be delivered by the Contractor to the Employer for his approval before the Start Date. All such insurance shall provide for compensation to be payable to rectify the loss or damage incurred. All payments received from insurers relating to loss or damage shall be held jointly by the Parties and used for the repair of the loss or damage or as compensation for loss or damage that is not to be repaired.

26.3 If the Contractor fails to effect or keep in force any of the insurances referred to in the previous sub- clauses or fails to provide satisfactory evidence, policies or receipts, the Employer may without prejudice to any other right or remedy, effect insurance for the cover relevant to such default and pay the premiums due and recover the same as a deduction from any other monies due to the Contractor. If no payment is due, the payment of the premiums shall be a debt due.

26.4 Alterations to the terms of insurance shall not be made without the approval of the Employer.

26.5 Both Parties shall comply with any conditions of the insurance policies.

C. Quality Control

27. Identifying defects

27.1 The Employer shall check the Contractor's work and notify the Contractor of any Defects that are found. Such checking shall not affect the Contractor's responsibilities. The Employer may instruct the Contractor to search for a Defect and to uncover and test any work that the Employer considers may have a Defect.

28. Tests

28.1 If the Employer instructs the Contractor to carry out a test not specified in the Specification to check whether any work has a Defect and the test shows that it has a defect, the Contractor shall pay for the test and any samples. If there is no defect, the testing charges shall be borne by the Employer.

29. Correction of Defects

29.1 The Employer shall give notice to the Contractor of any Defects before the end of the Defects Liability Period, which begins at Completion and is defined in the 'Appendix to Form of Tender'. The Defects Liability Period shall be extended for as long as Defects remain to be corrected.

29.2 Every time notice of a Defect is given, the Contractor shall correct the notified Defect within the length of time specified by the Employer's notice.

30. Uncorrected defects

30.1 If the Contractor has not corrected a Defect within the time specified in the Employer's notice, the Employer will assess the cost of having the Defect corrected, and the Contractor will pay this amount or will be recovered from any amount due to the Contractor from the Employer including Performance Security.

31. Inspections and Tests

31.1 The Employer or its representative shall have the right to inspect and/or to test the materials or works to confirm their conformity to the Contract specifications at no extra cost to the Employer. Special Conditions of Contract and the Technical Specifications shall specify what inspections and tests the Employer requires and where they are to be conducted. The Employer shall notify the Contractor in writing in a timely manner of the identity of any representatives retained for these purposes.

31.1 Should any inspected or tested materials fail to conform to the specifications, the Employer may reject the materials or Works and the Contractor shall either replace the rejected materials or make alterations /rectifications necessary to meet specification requirements free of cost to the Employer.

31.2 The Employer's right to inspect test and where necessary, reject the materials or Works at Project Site shall in no way be limited or waived by reason of the materials or Works having previously been inspected, tested and passed by the Employer or its representative prior to the dispatch of the materials.

31.3 Nothing in GCC Clause 31 shall in any way release the Contractor from any warranty or other obligations under this Contract.

32. Acceptance Certificates

On successful completion of acceptability test, receipt of deliverables etc, and after the Employer is satisfied with the completion of the Works, the Acceptance Certificate signed by the Contractor and the representative of the Employer will be issued. The date on which such certificate is signed shall be deemed to be the date of successful acceptance of the Works & will be considered as Go Live.

D. Cost Control

33. Bill of Quantities (BOQ)

33.1 The BOQ shall contain items for the Works including installation, testing, and commissioning work (if any) to be done by the Contractor.

33.2 The BOQ is used to calculate the Contract Price. The Contractor is paid for the quantity of the work done at the rate in the BOQ for each item.

34. Variations

34.1 The Employer shall have power to order the Contractor to do any or all of the following as considered necessary or advisable during the progress of the work by him
(a) Increase or decrease of any item of work included in the Bill of Quantities (BOQ);
(b) Omit any item of work;
(c) Change the character or quality or kind of any item of work;
(d) Change the levels, lines, positions and dimensions of any part of the work;
(e) Execute additional items of work of any kind necessary for the completion of the works; and

34.2 The Contractor shall be bound to carry out the work in accordance with any instructions in this connection, which may be given to him in writing by the Employer and such alteration shall not vitiate or invalidate the Contract.

34.3 Variations shall not be made by the Contractor without an order in writing by the Employer, provided that no order in writing shall be required for increase or decrease in the quantity of an item appearing in the BOQ so long as the work executed conforms to the approved drawings.

34.4 The Contractor shall not make any alteration and/or modification of the Works, unless and until the Engineer instructs or gives consent to a Variation.

If the Construction and/or Manufacture Documents or Works are not in accordance with the Contract, the rectification shall not constitute a Variation.

35. Payments for Variations

35.1 Payment for increase in the quantities of an item in the BOQ up to 25% of that provided in the Bill of Quantities shall be made at the rates quoted by the Contractor.

35.2 Under no circumstances the Contractor shall suspend the work on the plea of non-settlement of rates for items falling under this Clause.

36. Submission of bills for payment

36.1 The Contractor shall submit to the Employer monthly bills of the value of the work completed less the cumulative amount paid previously.

36.2 The Employer shall check the Contractor's bill and determine the value of the work executed which shall comprise of;

i) value of the quantities of the items in the BOQ completed and
ii) Valuation of Variations.

36.3. The Employer may exclude any item paid in a previous bill or reduce the proportion of any item previously paid in the light of later information.

37. Payments

37.1 Payments shall be adjusted for deductions for advance payments, if any, other recoveries in terms of Contract and taxes, at source, as applicable under the law. The Employer shall pay the Contractor within 60 days of submission of complete and valid Bill without any deficiency. The Contractor shall be liable to pay liquidated damages for shortfall in progress.

37.2 Items of the Works for which no rate or price has been entered in will not be paid for by the Employer and shall be deemed covered by other rates and prices in the Contract.

38. Not Used

39. Taxes & Duties

39.1 The Contract Price quoted by the Contractor shall be in accordance with the Special Conditions of the Contract and the Employer will perform such duties in regard to the deduction of taxes at source as per applicable law.

40. Liquidated damages

40.1 The Contractor shall pay liquidated damages to the Employer at the rate per day stated in the 'Appendix to Form of Tender' for each day that the Completion Date is later than the Stipulated Completion Date (for the whole of the Works or the milestone as stated in the 'Appendix to Form of Tender'). The total amount of liquidated damages shall not exceed the amount defined in the 'Appendix to Form of Tender'. The Employer may deduct liquidated damages from payments due to the Contractor. Payment of liquidated damages does not affect the Contractor's liabilities.

41. Cost of repairs

41.1 Loss or damage to the Works or Materials to be incorporated in the Works between the Start Date and the end of the Defects Liability Period shall be remedied by the Contractor at the Contractor's cost if the loss or damage arises from the Contractor's acts or omissions.

E. Finishing the Contract

42. Completion

42.1 The Contractor shall request the Employer to issue a Certificate of Completion of the Works and the Employer will do so upon deciding that the Work is completed.

43. Taking over

43.1 The Employer shall take over the Site and the Works within seven days of issuing a Certificate of Completion.

44. Final Bill / Account

44.1 The Contractor shall supply to the Employer a detailed account of the total amount that the Contractor considers payable under the Contract before the end of the Defects Liability Period. The Employer shall issue a Defect Liability Certificate and certify any final payment that is due to the Contractor within 90 days of receiving the Contractor's final bill / account, if it is correct and complete. If it is not, the Employer shall issue within 90 days a schedule that states the scope of the corrections or additions that are necessary. If the Final Bill / Account is still unsatisfactory

after it has been resubmitted, the Employer shall decide on the amount payable to the Contractor and make payment within 60 days of receiving the Contractor's revised Final Bill / Account.

45. "Operating and Maintenance Manuals"

45.1 Where "as built" / "Completion" Drawings and /or "Operating and Maintenance Manuals" are required, the Contractor shall supply them by the dates stated in the 'Appendix to Form of Tender'.

45.2 If the Contractor does not supply "Operating and Maintenance Manuals" by the dates stated in the 'Appendix to Form of Tender', or they do not receive the Employer's approval, the Employer shall withhold the amount stated in the 'Appendix to Form of Tender' from payments due to the Contractor.

46. Termination

46.1 The Employer may terminate the Contract if the Contractor causes a fundamental breach of the Contract.

46.2 Fundamental breaches of Contract include, but shall not be limited to the following:

(a) the Contractor stops work for 45 days when no stoppage of work is shown on the current Program and the stoppage has not been authorized by the Employer;

(b) The Contractor becomes bankrupt or goes into liquidation other than for a reconstruction or amalgamation;

(c) The Employer gives Notice that failure to correct a particular Defect is a fundamental breach of Contract and the Contractor fails to correct it within thirty (30) days of receipt of Notice of failure from BMRCL or within such further time period as BMRCL may have subsequently approved in writing;

(d) the Contractor does not maintain safety and security which is required;

(e) the Contractor has delayed the completion of works by the number of days for which the maximum amount of liquidated damages can be paid as defined in the 'Appendix to Form of Tender'; and

(f) if the Contractor, in the judgment of the Employer has engaged in corrupt or fraudulent practices in competing for or in the executing the Contract.

For the purpose of this paragraph:

(i) "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in Contract execution.

(ii) "Fraudulent practice" means any omission or misrepresentation of facts in order to influence a procurement process or the execution of a Contract to the detriment of the Borrower, and includes collusive practice among Tenderers (prior to or after Tender submission) designed to establish Tender prices at artificial non-competitive levels and to deprive the Borrower of the benefits of free and open competition."

46.3 When either party to the Contract gives notice of a breach of Contract to the Employer for a cause other than those listed under Sub Clause 46.2 above, the Employer shall decide whether the breach is fundamental or not.

46.4 Notwithstanding the above, the Employer may terminate the Contract for convenience.

46.5 If the Contract is terminated, the Contractor shall stop work immediately, make the Site safe and secure and leave the Site as soon as reasonably possible.

47. Payment upon Termination

47.1 If the Contract is terminated because of a fundamental breach of Contract by the Contractor, the Employer shall prepare bill for the value of the work done less advance payments received up to the date of the bill, less other recoveries due in terms of the Contract, less taxes due to be deducted at source as per applicable law and less the percentage to apply to the work not completed as indicated in the 'Appendix to Form of Tender'. Additional Liquidated Damages shall not apply. If the total amount due to the Employer exceeds any payment due to the Contractor, the difference shall be a debt payable to the Employer.

47.2 If the Contract is terminated at the Employer's convenience or because of a fundamental breach of Contract by the Employer, the Employer shall prepare bill for the value of the work done, the reasonable cost of removal of Equipment, repatriation of the Contractor's personnel employed solely on the Works, and the Contractor's costs of protecting and securing the Works and less advance payments received up to the date of the certificate, less other recoveries due in terms of the Contract, and less taxes due to be deducted at source as per applicable law and make payment accordingly.

48. Property

48.1 All materials on the Site, Plant, Equipment, Temporary Works and Works are deemed to be the property of the Employer, if the Contract is terminated because of a Contractor's default.

49. Release from performance

49.1 If the Contract is frustrated by any event entirely outside the control of either the Employer or the Contractor, the Employer shall certify that the Contract has been frustrated. The Contractor shall make the Site safe and stop work as quickly as possible after receiving this certificate and shall be paid for all work carried out before receiving it and for any work carried out afterwards to which commitment was made.

F. OTHERS

50. Warranty / Defects Liability Period

50.1 The Contractor warrants that all Works executed under this Contract shall have no defect arising from materials or workmanship (except when the material is required by the Employer's Specifications) or from any act or omission of the Contractor, that may develop under normal use of the supplied materials or the Works in the conditions prevailing in the country of final destination.

50.2 This Warranty shall remain valid for a period specified in Appendix to Form of Tender after the materials or Works or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the Contract. The Contractor shall, in addition, comply with the performance and/or consumption guarantees specified under the Contract. If for reasons attributable to the Contractor, these guarantees are not attained in whole or in part, the Contractor shall at its discretion either:

a) make such changes, modifications, and/or additions to the Works or any part thereof as may be necessary in order to attain the contractual guarantees specified in the Contract at

its own cost and expense and to carry out further Performance Tests in accordance to Special Conditions of Contract/Technical Specification; OR

b) pay liquidated damages to the Employer with respect to the failure to meet the contractual guarantees. The rate of these liquidated damages shall be as per GCC clause 40 or respective Special Conditions of Contract or as specified in the Technical Specifications.

50.3 The Employer shall promptly notify the Contractor in writing of any claims arising under this warranty.

50.4 Upon receipt of such notice, the Contractor shall, within the period of 3 days and with all reasonable speed, repair or replace the defective Works or parts thereof, free of cost at the ultimate destination. In the event of any correction of defects or replacement of defective material during the Warranty period, the Warranty for the corrected or replaced material shall be extended to a further period from the date of replacement/repair/renewal.

50.5 If the Contractor, having been notified, fails to remedy the defect(s) within 3 days, the Employer may proceed to take such remedial action as may be necessary, at the Contractor's risk and expense and without prejudice to any other rights which the Employer may have against the Contractor under the Contract.

51. Force Majeure

51.1 Notwithstanding the provisions of GCC Clauses 21, 22, 23, the Contractor shall not be liable for forfeiture of its Performance Security, liquidated damages or termination for default, if and to the extent that, its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

51.2 For purposes of this Clause, "Force Majeure" means an event beyond the control of the Contractor and not involving the Contractor's fault or negligence and not foreseeable. Such events may include, but are not limited to, acts of the Employer either in its sovereign or contractual capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

51.3 If a Force Majeure situation arises, the Contractor shall promptly notify the Employer in writing of such conditions and the cause thereof. Unless otherwise directed by the Employer in writing, the Contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

52. Claims, Disputes and Conciliation

Any and all Disputes shall be settled in accordance with the provision of this Clause.

52.1 Procedure for Claims

If the Contractor intends to claim any additional payment under any clause of these Conditions or otherwise, the Contractor shall give notice to the Engineer as soon as possible and in any event within 28 days of the start of the event giving rise to the claim.

The Contractor shall keep such contemporary records as may be necessary to substantiate any claim, either on the Site or at any other location acceptable to the Engineer. Without admitting the Employer’s liability, the Engineer shall, on receipt of such notice, inspect such records and may instruct the Contractor to keep further contemporary records. The Contractor shall permit the Engineer to inspect all such records, and shall (if instructed) submit copies to the Engineer.

Within 28 days of such notice, or such other time as may be agreed by the Engineer, the Contractor shall send to the Engineer a fully detailed claim which includes full supporting particulars of the basis of the claim and additional payment claimed. If the event or circumstance giving rise to the claim has a continuing effect:

(a) the initial fully detailed claim shall be considered as interim;
(b) the Contractor shall send further interim claims at monthly intervals, giving the cumulative amount claimed, and any such further particulars as the Engineer may reasonably require;
and
(c) the contractor shall send a final claim within 28 days after the end of effects resulting from the event or circumstance, or within such other period as may be proposed by the Contractor and approved by the Engineer.

If the Contractor fails to comply with this Sub-clause, he shall not be entitled to claim any additional payment.

52.2 Payment for Claims

The Contractor shall be entitled to have included in any Interim Payment Certificate such amount for any claim as the Engineer considers due, after taking approval from the Employer. If the particulars supplied are insufficient to substantiate the whole of the claim, the Contractor shall be entitled to payment for such part of the claim as has been substantiated

52.3 No Legal action till Dispute Settlement Procedure is Exhausted

Any and all Disputes shall be settled in accordance with the provisions of Clause 52. No action at law concerning or arising out of any Dispute shall be commenced unless and until all applicable Dispute resolution procedures set out in Clause 52 shall have been finally exhausted in relation to that Dispute or any Dispute out of which that Dispute shall have arisen with which it may be or may have been connected.

52.4 Notice of Dispute

A Dispute shall be deemed to arise when one party serves a notice in writing (hereinafter called a "Notice of Dispute") within 30 days from the date of rejection of claim by the parties.

52.5 Dispute Resolution

Disputes shall be settled through Conciliation procedures as established by “The Arbitration and Conciliation Act, 1996” and as amended from time to time.

52.6 Conciliation

Within 60 days of receipt of Notice of Dispute, either party shall refer the matter in dispute to conciliation. Conciliation proceedings shall be initiated within 30 days of one party inviting the other in writing to Conciliation. Conciliation shall commence when the other party accepts in writing this invitation. If the invitation is not accepted, then Conciliation shall not take place. If the party initiating conciliation does not receive a reply within 30 days from the date on which he sends the invitation, he may elect to treat this as a rejection of the invitation to conciliate and inform the other party accordingly.

The Conciliation shall be undertaken by one Conciliator selected from a panel of Conciliators maintained by the Employer. The Conciliator shall assist the parties to reach an amicable settlement in an independent and impartial manner.

52.7 Conciliation Procedure

The Employer shall maintain a panel of Conciliators with requisite qualifications and professional experience who shall be from serving or retired engineers of Government Departments, or of

Public Sector Undertakings. Panel list not to include serving or former employees of the Employer. Out of this panel, a list of three Conciliators shall be sent to the Contractor who shall choose one of them to act as Conciliator and conduct conciliation proceedings in accordance with "The Arbitration and Conciliation Act, 1996", of India. The party serving notice of dispute on the other party shall also serve such notice on the Conciliator chosen as per this Clause. The Employer at the time of offering the panel of Conciliators to be appointed as Conciliator shall also supply the information with regard to the qualifications of the said Conciliators nominated in the panel along with their professional experience, phone nos. and addresses to the Contractor.

In the event of the Contractor not choosing the Conciliator from the panel furnished by the Employer, within a period of 30 days, the Employer is at liberty to choose and nominate a Conciliator from the same panel and communicate to the Contractor which will be final and binding on the Contractor.

The Employer and the Contractor shall in good faith co-operate with the Conciliator and, in particular, shall endeavour to comply with requests by the Conciliator to submit written materials, provide evidence and attend meetings. Each party may, on his own initiative or at the invitation of the Conciliator, submit to the Conciliator suggestions for the settlement of the dispute.

When it appears to the Conciliator that there exist elements of a settlement which may be acceptable to the parties, he shall formulate the terms of a possible settlement and submit them to the parties for their observations. After receiving the observations of the parties, the Conciliator may reformulate the terms of a possible settlement in the light of such observations.

If the Parties reach agreement on a settlement of the dispute, they may draw up and sign a written settlement agreement. If requested by the Parties, the Conciliator may draw up, or assist the Parties in drawing up, the settlement agreement.

When the Parties sign the settlement agreement, it shall be final and binding on the parties and persons claiming under them respectively.

The Conciliator shall authenticate the settlement agreement and furnish a copy thereof to each of the Parties.

To the fullest extent feasible, the conciliatory process must be concluded within a period of sixty days subsequent to the acknowledgment of the appointment notice by the Conciliator.

The Parties shall not initiate, during the conciliation proceedings, any judicial proceedings in respect of a dispute that is the subject matter of the conciliation proceedings.

52.8 Termination of Conciliation Proceedings

The conciliation proceedings shall be terminated:

a. by the signing of the settlement agreement by the Parties on the date of agreement; or

b. by written declaration of the Conciliator, after consultation with the Parties, to the effect further efforts at conciliation are no longer justified, on the date of declaration; or

c. by a written declaration of the Parties to the Conciliator to the effect that the conciliation proceedings are terminated, on the date of declaration; or

d. by a written declaration of a Party to the other Party and the Conciliator, if appointed, to the effect that the conciliation proceedings are terminated, on the date of declaration.

Upon termination of the conciliation proceedings, the Conciliator shall fix the costs of the conciliation and give written notice thereof to the Parties. The costs shall be borne equally by the Parties unless settlement agreement provides for a different apportionment. All other expenses incurred by a Party shall be borne by that Party.

52.9 Suspension of Work on Account of conciliation

The reference to Conciliation shall proceed not withstanding that the Works shall not then be or be alleged to be complete, provided always that the obligations of the Employer, Engineer and the Contractor shall not be altered by reasons of conciliation being conducted during the progress of the Works. Neither party shall be entitled to suspend the work or part of the work to which the

dispute relates on account of conciliation and payments to the Contractor shall continue to be made in terms of the Contract.

52.10 Judicial Recourses

In the event that a dispute remains unresolved via the conciliation process, the aggrieved party may seek judicial recourses.

52.11 Jurisdiction of Courts

Any suit or application, arising out of any dispute or differences on account of this contract shall be filed in a competent court at Bangalore, Karnataka only and no other court or any other district of the country shall have any jurisdiction in the matter.

52.12 Matters finally determined by the Employer

If the Contractor (s) does/do not prefer his/ their specific and final claims in writing, within a period of 90 days of receiving the intimation from the Employer that the final bill is ready for payment, he/they will be deemed to have waived his/their claims (s) and the Employer shall be discharged and released of all liabilities under the contract in respect of these claims

53. Patent Rights

53.1 The Contractor shall indemnify the Employer against all third-party claims of infringement of Intellectual Property rights of patent, trademark or industrial design rights arising from use of the materials or design or data or any part thereof in India.

54. Limitation of Liability

54.1 Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to GCC Clause 53,

a) The Contractor shall not be liable to the Employer, whether in Contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Contractor to pay liquidated damages to the Employer; and

b) The aggregate liability of the Contractor to the Employer, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective works / equipment.

55. Governing Language

The Contract shall be written in English language. Subject to GCC Clause 3, English language version of the Contract shall govern its interpretation. All correspondence and other documents pertaining to the Contract, which are exchanged by the parties, shall be written in the same language.

56. The Courts of Jurisdiction

56.1 Any suit or application, arising out of any dispute or difference on account of this Tender shall be filed in a competent court at Bengaluru, Karnataka only and no other court or any other district of the country shall have any jurisdiction in the matter.

57. Notices

57.1 Any notice given by one party to the other pursuant to this Contract shall be sent to other party in writing or by facsimile or cable or telex or by hand (duly acknowledged) and confirmed in writing to the other Party's address specified in Special Conditions of Contract.

58. Use of Contract Documents and Information; Inspection and Audit by the Government

58.1 The Contractor shall not, without the Employer's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Employer in connection therewith, to any person other than a person employed by the Contractor in performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

58.2 The Contractor shall not, without the Employer's prior written consent, make use of any document or information enumerated in GCC Clause 58.1 except for purposes of performing the Contract.

58.3 Any document, other than the Contract itself, enumerated in GCC Clause 58.1 shall remain the property of the Employer and shall be returned (in all copies) to the Employer on completion of the Contractor's performance under the Contract if so required by the Employer.

58.4 The Contractor shall permit BMRCL to inspect the Contractor’s accounts and records relating to the performance of the Contractor and to have them audited by Auditors appointed by the BMRCL, if so required by BMRCL.

--- XXX ---

SECTION 6: SPECIAL CONDITIONS OF CONTRACT

1. General

The following Special Conditions shall be read in conjunction with the Section 5: General Conditions of Contract including Amendments/ Corrigendum thereto. If any provision in these Special Conditions is at variance with that of the aforesaid documents, the later shall be deemed to take precedence there over.

2. Subcontracting

Prior approval of the Employer shall be obtained before sub-contracting any part of the works. However, the Contractor shall not subcontract the whole of the Works. The Tenderer shall Submit the details of Sub-Contractors to the Employer for approval.

3. Access to the Site (GCC Clause 19)

Security and Passes:

3.1 Contractor's attention is invited to condition that, he shall employ only Indian Nationals after verifying their antecedent and loyalty. The Contractor shall, maintain list of his agents, employees and work people concerned and shall satisfy the Engineer as to the bonafides of such people, and submit to the Engineer / Employer on demand.

3.2 The Employer shall at his discretion have the right to issue passes as per rules and regulations of the installation, area in force to control the admission of the Contractor, his agents employees and work people to the site of the work or any part thereof. Passes should be returned at any time on demand by the Engineer or the authorities concerned and, in any case on completion of work.

3.3 The Contractor and his agents, employees and workers shall observe all the Rules promulgated by the authority controlling the installation area in which the work is to be carried out. e.g. Prohibition of smoking and lighting, fire precautions, search of persons on entry and exit, keeping to specific route, observing specified timing, etc., nothing extra shall be admissible for any man hours, etc., lost on this account.

3.4 **Conditions of working in restricted area:**

Work under this Contract lies in restricted area.

3.4.1 **Visit to site within the restricted area**

Permission to enter the restricted areas at the time of submission of Tenders can be obtained through the Employer or his authorized Representative. Tenderers are advised to send prior intimation of their agents, representatives etc., if any, dates and time of their proposed visit so that necessary arrangements may be made by Employer to secure admission. Whether a Tenderer visits the site or not he shall be deemed to have full knowledge of the restriction of entering into/exit from and working within the restricted area.

3.4.2 **Entry/Exit**

The Contractor, his agents/representatives, workmen etc., and his materials, carts, trucks or other means of transport etc., will be allowed to enter through and leave from only such gate or gates and such times as the employer or authorities in charge of the restricted areas may at their sole discretion permit to be used. The Contractor's authorized representatives are required to be present at the place of entry and exit for the purpose of identifying his carts, trucks etc., to the personnel in charge of the security of restricted areas.

3.4.3 **Identity Cards or Passes**

The Contractor, his agents and representatives are required individually to be in possession of an identity Card or Pass duly verified by the Employer or his authorized Representative. The identity card or pass will be examined by the Security Staff at the time of entry into or exit from the Restricted Area and also at any time or number of times inside the Restricted Area.

3.4.4 **Identity of Workmen**

(i) Every workman shall be in possession of an identity card. The Identity Card will be issued after thorough investigation of the antecedents of the labourers by the Contractors and attested by Officer-in-Charge of the unit concerned in accordance with the Standing Rules and regulations of the units.

(ii) Contractor shall be responsible for the conduct and action of his workmen, agents or representatives.

3.4.5 **Search**

Thorough search of all persons and transport shall be carried out at each gate and for as many times as the gate is used for entry or exit and may also be carried out at any time or any number of times at the work site within the Restricted area.

3.4.6 **Working Hours**

The SOC will be operational on all the 365 days of the calendar year (24x7 basis)

3.4.7 Co-operation with other Agencies:

The Contractor shall permit free access and generally afford reasonable facilities to other agencies or departmental workmen engaged by the BMRCL to carry out their part the work, if any, under separate arrangements.

3.4.8 **Electric Supply**

Electricity shall be provided on chargeable basis considering the unit rate charged by BESCOM to BMRCL (i.e. based on the prevailing rate/s of BESCOM), if available and feasible. Otherwise, the Contractor shall make his own arrangements at his own cost, for Electrical Power and gas required for his works. Work shall not be delayed for non-availability of electricity/gas.

3.4.9 **Emergency Works**

If, by reason of an emergency arising in connection with and during the execution of the Contract, any protective or remedial work is necessary as a matter of urgency to prevent damage to the Facilities, the Contractor shall immediately carry out such work, under intimation to the Engineer.

4. Inspections and Tests (GCC Clause 31)

4.1. **Inspections and tests at final acceptance are as follows:**

(i) The inspection of the materials / Works shall be carried out to check whether the materials / Works are in conformity with the Technical Specifications attached to the Contract and shall be in line with the inspection/test procedures laid down in the Technical Specifications and the General Conditions of Contract. Following broad test procedure will generally be followed for inspection and testing of works.

(ii) The acceptance test will be conducted by the Contractor in presence of the Employer/ Engineer / their representative or any other person nominated by the Employer / Engineer. The acceptance will involve trouble-free operation. There shall not be any additional charges for carrying out acceptance tests. No malfunction, partial or complete failure of the Works should occur.

(iii) In the event of the materials / Works failing to pass the acceptance test, a period not exceeding two weeks will be given to rectify the defects and clear the acceptance test, failing which the Employer reserves the rights to get the Works replaced / redone by the Contractor at no extra cost to the Employer.

5. Variations (GCC Clause 34)

Total variation under the Contract shall be limited to ± 25% of the Total Original Value of the Contract.

6. Payments for Variations (GCC Clause 35)

Payments for variations shall be made in accordance to GCC Clause 35.

7. Taxes and Duties (GCC Clause 39)

7.1 The Contract price shall be inclusive of all applicable Taxes, Cess and duties under the applicable Acts but exclusive of GST. The GST will be paid as applicable as per law.

7.2 **Income Tax (IT) deduction:** As per the prevailing rate, IT shall be deducted and remitted to the Income Tax authorities and Form 16 shall be furnished by BMRCL in proof of remittance to IT Department. For availing lower deduction of Income Tax, necessary certificate for each financial year issued by the Income Tax Authority shall be furnished by the Contractor, failing which IT at the maximum rate will be deducted.

7.3 The Contract Price shall be inclusive of all charges of insurance, transportation up to destination, handling, installation, royalties & any other charges leviable and payable by the Contractor under the Contract, or for any other cause and including Tax to be deducted at source and shall be included in the Total Tender Price.

7.4 The Contractor shall be entirely responsible for license fees and any other incidentals incurred until completion of the whole of the Works and handover to the Employer.

7.5 The Contractor shall maintain complete records of duties, other taxes and levies, etc; payable to various authorities in relation to the Works and submit the receipts/records for verification as and when demanded in writing by the Employer.

7.6 Any increase in GST shall not be paid in the extended period of Contract for which the Contractor alone is responsible for delay as determined by the Engineer while granting the extension of time". However, this shall not be applicable for "Variations".

8. Termination (GCC Clause 46)

8.1 The Fundamental breach of the Contract shall also include that "the Contractor has contravened SCC Clause 3 (Subcontracting) and GCC Clause 9 (Personnel).

8.2 In the event the Employer terminates the Contract in whole or in part, pursuant to GCC Clause 46, the Employer;

(i) shall forfeit the performance Security, and

(ii) may carry out the Works, upon such terms and in such manner as it deems appropriate, Works similar to those incomplete, and the Contractor shall be liable to the Employer for any excess costs for such similar Works. However, the Contractor shall continue the performance of the Contract to the extent not terminated.

9. Not Used

10. Notices (GCC Clause 57)

For the purpose of all notices, the following shall be the address of the Employer and Contractor.

Employer:

Bangalore Metro Rail Corporation Limited
3rd Floor, BMTC Complex (C-Block),
K.H.Road, Shanthinagar,
Bangalore, PIN 560 027
Karnataka, India

Contractor:

…….
(To be filled in after the award of Contract).

11. Use of Contract Documents and Information; Inspection and Audit by the Government (GCC Clause 58)

11.1 **Security of Classified Documents:**

The Contractor shall not communicate any classified information regarding work to others without prior approval of Engineer. The Contractor shall also not make copies of the design/drawings and other documents furnished to him in respect of works and he shall return all documents after completion of works or on earlier determination of Contract. The Contractor shall along with final bill, attach a receipt from the Engineer in respect of his having returned the classified documents as per condition of General Conditions of Contract.

12. Protection of Environment (New Clause)

12.1 The Contractor shall take all reasonable steps to protect the environment on and off the Site and to avoid damage or nuisance to persons or to property of the public or others resulting from pollution, noise or other causes arising as a consequence of his methods of operation. During continuance of the Contract, the Contractor and his Subcontractors shall abide at all times by all existing enactments on environmental protection and rules made there under, regulations, notifications and bye-laws of the State or Central Government, or local authorities and any other law, bye-law, regulations that may be passed or notification that may be issued in this respect in future by the State or Central Government or the local authority.

13. Certification of Local Content:

During execution of the Contract, in case the Contractor does not meet the stipulated Local Content requirement and the category of the Contractor changes from Class-I to Class-II/ Non-local or from Class-II to Non-local, a penalty up to 10% of the Contract Price shall be imposed. Therefore, to ensure this, the Employer will hold 10% of the Contract Price, if the condition of certification of Local Content has not been met by the Contractor.

Alternatively, the Contractor can submit a Bank Guarantee (in line with PBG) for an amount of 10% of the Contract Price till the condition of certification of Local Content is met for release of due payment out of 10% payment. In such cases, the cost of the BG charges shall be borne by the Contractor.

--- xxx ---

SECTION 7 – TECHNICAL SPECIFICATIONS

Abbreviations

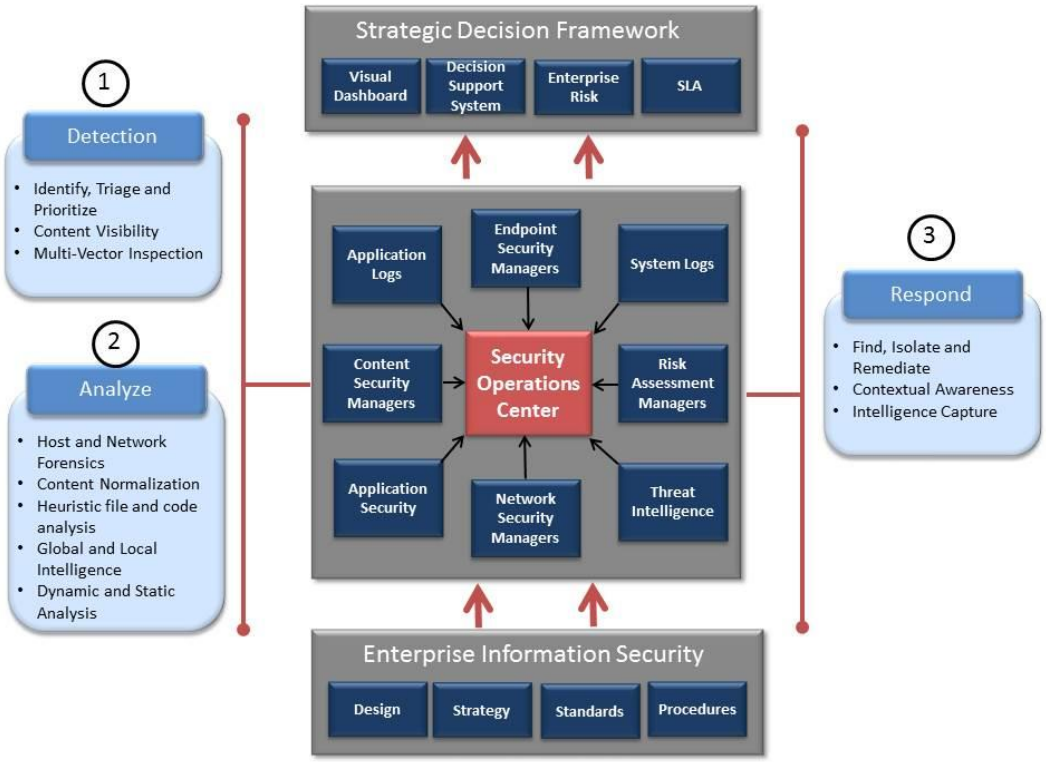
- KSWAN: Karnataka State Wide Area Network
- SOC: Security Operations Center
- NOC: Network Operations Center
- OEM: Original Equipment Manufacturer
- O&M: Operations & Maintenance
- EMS: Enterprise Management Suite
- NMS: Network Monitoring System
- EMD: Earnest Money Deposit
- PBG: Performance Bank Guarantee
- SLA: Service Level Agreement
- TPA: Third Party Agency
- SoW: Scope of Work
- SIEM: Security Information and Event Management
- SOAR: Security Orchestration, Automation and Response
- UEBA: User and Entity Behavior Analytics
- CCTV: Closed Circuit Tele Vision
- QP: Quarterly Payment
- IAM: Identity and Access Management
- RBAC: Role-Based Access Control

Section I: Introduction

1. Security Operations Center (SOC)

BMRCL has decided to establish a Security Operations Center (SOC). The SOC will monitor, prevent, assess, detect, respond to, and defend BMRCL's critical information systems and IT infrastructure against cyber threats. This includes the integration and commissioning of an on-premises SOC for IT and CCTV networks of the Bangalore Metro Rail Project. The operation and maintenance of the SOC will extend for three years after going live. The SOC will also ensure the health monitoring and uptime availability of the entire CCTV network and the network operations center (NOC) for surveillance purposes.

The interconnections among diverse actors, networks, applications, systems, and computing devices create a web of interdependencies. The health of one component can impact the entire ecosystem. Developing an effective SOC requires recognizing and understanding this environment. An unprotected computer can expose numerous trusted networks; a successful Denial-of-Service attack can slow or interrupt services across the IT infrastructure. If unchecked, malware could spread like a pandemic through the environment. While these interconnections can create vulnerabilities, they also allow SOC to operate effectively by collaborating to gather and analyze information and respond to attacks. Effective SOC operations require monitoring, holistic threat detection, the right cyber security skills, analyzing multiple devices and logs, intelligent incident detection and response, and centralized forensic capabilities.



Detection stage: a Security Operations Center (SOC), data is collected from various sources through agents and sent to a centralized server. This data undergoes parsing and normalization for consistent analysis. Correlation rules and threat intelligence feeds are then applied to identify potential security events. Detection methods include anomaly detection, signature-based detection, and behavioral analysis. When a threat is detected, alerts are generated and categorized by severity. BMRC Security analysts investigate these alerts to confirm their validity and take appropriate actions to mitigate threats. Detailed reports and documentation of incidents are created, and continuous improvements are made by updating detection rules and incorporating lessons learned.

Analysis stage: security analysts delve into the alerts generated during detection. They examine detailed logs and event data to understand the context and legitimacy of the detected threats. Analysts use various tools and techniques to correlate events, identify patterns, and assess the potential impact of the threat. They prioritize incidents based on severity and relevance, ensuring that critical threats are addressed promptly. Throughout this process, the analysts aim to determine the root cause of the incident, identifying vulnerabilities and attack vectors. The analysis helps in formulating an appropriate response and in updating security measures to prevent future incidents. Continuous monitoring and refined threat intelligence play a crucial role in enhancing accuracy and efficiency.

Remediation stage: actions are taken to neutralize and resolve identified threats. Security analysts collaborate with BMRCL IT teams to implement measures such as patching vulnerabilities, isolating compromised systems, and removing malicious software. Detailed remediation plans are developed to ensure that all aspects of the threat are addressed, and the system is restored to a secure state. Communication with stakeholders is maintained to keep them informed about the actions taken and the progress made. Post-remediation, a review is conducted to evaluate the effectiveness of the response and to identify any gaps or areas for improvement. Lessons learned from the incident are incorporated into future incident response strategies.

Monitoring stage: continuous surveillance of the network and systems is maintained to detect any signs of recurring or new threats. Advanced monitoring tools and techniques are employed to ensure real-time visibility and prompt detection of anomalies. Security analysts regularly review logs, alerts, and performance metrics to identify patterns and trends that may indicate potential security issues. Ongoing threat intelligence feeds and updates to detection rules help in adapting to the evolving threat landscape. Regular audits and assessments are conducted to ensure compliance with security policies and standards. The monitoring stage is crucial for maintaining a proactive security posture and ensuring the long-term protection of the BMRCL assets.

Section II: Scope of Work

BMRCL has issued this Tender for Establishment and Management of on-premises Security Operation Center (24x7x365 days) at BMRCL.BMRCL envisages setting up of SOC at Baiyappanahalli,

1.1. Establishment and Management of on-premises SOC:

1.1.1 Bidder is required to supply, install, configure, test and commission the required Hardware, software and compute (inclusive of all active & passive components and subcomponents, accessories) as per the technical and functional specification mentioned in the Tender document.

1.1.2 The licenses supplied by the selected bidder should be in the name of BMRCL valid perpetual for life and handover to BMRCL.

1.1.3 Bidder is required to provide Racks with PDU & other components

1.1.4 Required Power point within each rack will be provided by BMRCL. However, bidder will have to ensure that the hardware supplied/delivered is compatible with the PDU's supplied in the rack or bidder needs to provide required connector, if any.

1.1.5 The bidder should provision the required hardware and software components which mentioned in the Tender to be implemented under this Tender Scope.

1.1.6 The Bidder has to ensure that if any additional component(s) required for overall solution to comply with the implementation to achieve desired objectives and SLA levels, then in such case it should be the responsibility of the bidder to provide the same as a part of the entire solution.

1.1.7 The architecture needs to be scalable to meet future demand.

1.1.8 Bidder shall be responsible for setting up of on premise SOC at BMRCL premises and provide the required security services for period of 3 years. The delivery model of 24/7 SOC should be hybrid including Onsite and remote SOC resources (People, Process and Technology) required to run and manage the SOC shall be provisioned from the bidder's own sources to manage, monitor, analyze and report incidents as they occur.

1.1.9 The requirements in the Security Operations Centre (SOC) shall at the minimum include the

following functionalities/capabilities. Accordingly, the bidder shall: A NEXT-GEN ON-PREM & CLOUD SECURITY PLATFORM THAT HAS A SIEM and analytics IN-BUILT INTO A SINGLE, COHESIVE SYSTEM. It integrates seamlessly with next gen SOAR. It provides end-to-end security analysis, intrusion detection, log data analysis, incident response, regulatory compliance and more.

1.1.10 It SHOULD combines data from Multiple sources and provides A feature packed, Vendor Agnostic, Enterprise ready **SOC** Platform built with Artificial Intelligence, Machine Learning and threat hunting friendly platform.

1.1.11 Build custom interfaces if required for integration

1.1.12 Provide Security Intelligence for SOC Solutions

1.1.13 Provide post implementation monitoring & management support.

1.1.14 Integrate any other device procured by the BMRCL.

1.1.15 Provide monitoring services in hybrid mode for

- 24x7x365 Real-time Security Monitoring in a Fully Managed Service Delivery Model
- Correlation of event logs with other relevant security information including vulnerability information, network flows and external threat intelligence
- Leverage the SIEM solution detect, analyze, and qualify security alerts for various use-cases
- Escalate qualified security incidents to BMRCL for further investigation.
- Create incident tickets in a ticketing tool for the qualified incidents and alerts.
- Analyze false positives and recommend modification/deletion of correlation rules.
- Provide remediation recommendations.
- 24x7x365 SOC Tools & SOC Infrastructure Administration and Support in a Co-Managed Service Delivery Model
- The Bidder should provide – remote SOC monitoring &management services on 24 x 7 x 365 basis for the entirety of the contract period of 3 years. Bidder should provide two SOC L1 resources onsite for program management and to ensure end to end closure of the incident tickets.
- The bidder should make at least five L1 , three L2 and one L3 resources available for BMRCL including skilled SME's on the solutions deployed in BMRCL and soc scope.
- The bidder should provide service desk access to BMRCL SOC team and at least five technician licenses for BMRCL use.
- The SOC services should include Threat hunting and Cyber Threat Intel collection, curation and sharing actionable intel feeds to BMRCL SOC team. Bidder should share security advisories specific to BMRCL.
- Perform Health and Availability monitoring and notification of the SOC solution
- Perform Validation of successful configuration backup and log archival based on BMRCL policies

1.1.20 Provide single integrated and consolidated enterprise view of security and compliance in the dashboard

1.1.21 Provide roll-out plans for each of the deliverable and adhere to the same

1.1.22 Bidder to design and implement the complete security policy and workflow as per industry best practice in consultation with SOC -BMRCL IT TEAM to meet their business requirements.

1.1.23 Warranty Support: As part of the warranty services bidder shall provide:

1.1.24 Bidder shall provide a comprehensive on-site and free warranty for 3 years from the date of Go-Live for proposed solution

1.1.25 Warranty and Support of all devices & tools will be considered only after successful installation.

1.1.26 Bidder shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the bid.

1.1.27 During the warranty period bidder, shall maintain the systems and repair / replace at the installed site, at no charge, all defective components that are brought to the bidder notice.

1.1.28 The bidder shall as far as possible repair/ replace the equipment at site.

1.1.29 Warranty should not become void, if BMRCL buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the bidder. However, the warranty

will not apply to such supplemental hardware items installed.

1.1.30 Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

1.1.31 Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

1.1.32 Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

1.1.33 To provide warranty support effectively, OEM should have spare depo in India and will be asked to deliver spare as per SLA requirement.

1.1.34 "After completion of 3 years warranty/CAMC period, if required, BMRCL may extend the warranty/CAMC support for further period of 2 years (4th year and 5th year) on the derived rates of average cost of 3 years warranty/CAMC cost quoted. Bidder is required to provide the undertaking for the same mentioning that they will provide 5th year and 6th year warranty/ CAMC support".

1.1.35 The Bidder shall ensure that the products quoted should not be declared "End of Production" for next 3 years and "End of support" for the next 5 years by the OEM from the date of bid submission. However, if OEM declares any equipment/solution/software/or part as end of support for any reasons, then in that case OEM has to replace that equipment with better or equivalent products without any cost to BMRCL OEM to provide compliance on their letter head for the specification of Hardware and Software Infrastructure

1.2 Key Deliverables:

The bidder needs to provide following deliverables in accordance with the Implementation Timelines.

S/N	Deliverables	Activity
1.	Kick-off meeting	• Project Plan
2.	Delivery of Components	• Software License documents • Hardware warranty certificate
3.	Installation & Commissioning	• Solution architecture documents • Logical and physical design • Completion of UAT and closure of observations • Integration Testing Report • Test cases & SOPs for the SOC
4.	Go Live	• Successful implementation of SOC solution specifications and functional requirements as mentioned in this RFP
5.	Deployment of manpower proposed for O&M of SOC	• Required Manpower as per scope of RFP

1.3 Bill of Material

The tenderer is intended to procure following system included but not limited to required Hardware, Software, License, Accessories and any other device / software to full fill the functional requirement mentioned under this RFP.

S.No.	Description (including software, licenses, warranty, CAMC, services) for 3 years	UoM	Qty.
1	SIEM/SOC Security platform	Set	1
2	24/7 SOC Services in hybrid model	Set	1
3	SOAR platform with 10 technician licenses	Set	1
4	UEBA	Set	1
5	NOC for CCTV Network	Set	1
6	Cyber Security Posture Assessment	Set	1
7	A dedicated SOC Analysts (L1) onsite as per above scoped assets for 3 years	Set	2
8	AMC-24x7 Managed SOC service of Ecosystem	Set	1
9	One time deployment charges of software components installation and configuration	Set	1
10	Two LED TV's 85''	No.	2
11	Workstation with dual monitor	No.	2

Section III: Technical Specification

The bidder should provide state of the art solution to fulfil over all functional requirement for SOC. Services to be offered to BMRCL:

1. Monitoring and Log Analysis Services

1.1.1 The devices included in the scope of monitoring & log analysis to be carried out from the SOC to be set up in the BMRCL's Premises and managed by the Bidder's personnel are as follows:

1.1.2 On-premises implementation of SOC ecosystem with integrated SIEM, Threat Intel, Compliance reporting and SOAR. Integrate all log sources in scope with siem and enabke and create SOAR playbooks.

1.1.3 Management of Security devices deployed as per the scope of setting up the Security Operations Center including rule base audit and management of devices creation of rules during non-business hours. Monitoring of 24x7 logs & audit trails for the security events to detect known as well as unknown attacks and raising alerts on any suspicious events that may lead to security breach into BMRCL's environment. Monitoring of 24x7 performance and service availability so that the desired state and integrity of the devices and services levels are maintained.

1.1.4 To be able to support and provide scalability for any additions/modifications or integration of applications, services, devices and networks with the existing architecture.

1.1.5 Impact Analysis of any suspicious traffic and initiating response in co-ordination with the BMRCL's IT team

1.1.6 Providing initial review (Level 1) of security incidents and the determination if escalation to Level 2, 3 supports is warranted.
1.1.7 Creation and adding custom correlation rules for the BMRCL's devices under scope. BMRCL will review and fine-tune rules as and when required.
1.1.8 Monitoring alerts and events reported by devices under the SOC scope; to record the incidents, classify, and recommend remedial action. All types of incidents will have to be reported immediately as per the escalation matrix.
1.1.9 Initiation of prompt corrective countermeasures to stop/prevent attacks as per predetermined procedures.
1.1.10 Complete analysis and correlation of logs from all the devices under scope.
1.1.11 Carrying out due forensic activities to identify the origin of threat, mitigation steps and measures to prevent recurrence.
1.1.12 Preparation of the daily/ weekly / monthly reports to summarize the list of incidents, security advisories, and other security recommendations. It should include the operations trend analysis with the reports correlation of the present month's operations data with the previous months' data.
1.1.13 strengthen their ability to detect and protect against advanced threats

2. Malware Detection
2.1.1 Real-time Cross-Platform Protection: Detect and block malware across different operating systems instantly.
2.1.2 Ransomware Protection: Prevent ransomware attacks by detecting malicious encryption activities.
2.1.3 Rootkit Detection: Identify and remove hidden malware that gains privileged access.
2.1.4 Extensible Integrations for Malware Detection: Seamlessly integrate with other security tools for enhanced detection capabilities.
2.1.5 Advanced Rulesets and Decoders: Use sophisticated algorithms to identify and decode malware patterns.
2.1.6 Centralized Threat Visualization: Display threat data in a unified view for better analysis.

3. Threat Intelligence
3.1.1 Comprehensive Visibility: Gain an all-encompassing view of potential threats.
3.1.2 Log Retention, Indexing, and Query: Store and search through logs for threat analysis.
3.1.3 MITRE ATT&CK Mapping: Align security measures with a globally recognized framework.
3.1.4 Threat Intelligence: Leverage up-to-date data on emerging threats.
3.1.5 Tailored Ruleset: Customize detection rules to suit organizational needs.
3.1.6 Command Monitoring: Watch for suspicious command executions.
3.1.7 Customizable Dashboard: Personalize the interface for optimal use.

4. Log Data Analysis
4.1.1 Security Threat Detection: Analyze logs to identify potential threats.
4.1.2 Regulatory Compliance: Ensure log data meet compliance requirements.
4.1.3 Seamless Integration with Third-Party Solutions: Facilitate smooth incorporation with existing tools.
4.1.4 Holistic View of Entire IT Infrastructure: Provide a comprehensive perspective on IT operations.
4.1.5 Scalability and Performance: Support growth and maintain performance.
4.1.6 Host-Based Intrusion Detection System (HIDS): Monitor individual hosts for intrusions.

5. Incident Response
5.1.1 Automated Incident Response: React to incidents with minimal human intervention.
5.1.2 SOAR workflows should be configured to triage, respond and remediate suitable alerts.
5.1.3 SOAR should act as single source of truth for all IR activities supporting with data enrichment, external look ups, case management, notifications, contributing events and remediations.
5.1.4 Streamlined Operations: Simplify the incident management process.
5.1.5 Third-Party Integrations: Connect with other security tools to enhance response capabilities.
5.1.6 Reduced Dwell Time: Minimize the time attackers spend in your environment.

5.1.7 IR plan should be in line with global standards.

6. Regulatory Compliance
   - 6.1.1 Audit Infrastructure: Regularly review systems to meet compliance standards.
   - 6.1.2 Streamline Compliance Activities: Ease the process of maintaining compliance.
   - 6.1.3 Support for Various Compliance Standards: Adhere to multiple regulatory frameworks.
   - 6.1.4 Create Custom Policies and Security Controls: Develop specific guidelines tailored to organizational needs.
   - 6.1.5 Generate Compliance Reports: Produce necessary documentation for regulatory bodies.

7. Cyber Security Posture Assessment
   - 7.1.1 Bidder should carry out cyber security posture assessment for BMRCL IT Infrastructure in line with NIST CSF.
   - 7.1.2 The posture assessment should Ascertain BMRCL cyber security program's **current profile** (where the organization stands at the time of the assessment relative to each control) and **target profile** (where the organization would like to be at some future date relative to each control).
   - 7.1.3 **The assessment report should** Use identified weak spots in BMRCL cyber security program to build a roadmap to strengthen customer cybersecurity posture
   - 7.1.4 The assessment report should be simple and Communicate with visual dashboards understood by non-technical leadership
   - 7.1.5 The assessment report should list all the gaps, blind spots and Cyber risks that leave BMRCL exposed.
   - 7.1.6 The assessment should include SME Driven approach also for assessment for validation and to reduce subjectiveness
   - 7.1.7 The assessment report should give detailed recommendations to mitigate the gaps identified with proper prioritisation.

8. SOC Use Case
   - 8.1.1 Monitoring USB drives in Windows
   - 8.1.2 Monitoring Windows Task Scheduler for attack persistence
   - 8.1.3 Monitoring commonly abused Windows utilities
   - 8.1.4 Monitoring Windows resources using Performance Counters
   - 8.1.5 Utilizing OSINT for CDB lists and blocking malicious Ips
   - 8.1.6 Monitoring root actions on Linux
   - 8.1.7 Monitoring remote OpenVPN connections with GeoIP
   - 8.1.8 Create use cases based on Security essentials, based on business logic, device based etc.
   - 8.1.9 SOC use cases in line with MITRE framework across the TTP's.

9. Dashboard View:
   - 1.1 The bidder shall provide a SOC a single dashboard view of all the integrated devices, tools, applications, and databases for ease of monitoring
   - 1.2 The Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department.
   - 1.3 The Dashboard should support export of data to multiple formats including CSV, XML, Excel, PDF, word formats Dashboard should accept CSV, XML, Excel formats to upload data in the dashboard SLA data should be captured in the dashboard with compliance details

10. SOC Operations Team Specification

10.1 The asset list and service deliverables are provided in this Tender for the bidder to assess the volume of work and accordingly provide adequate personnel with appropriate skills. The minimum team structure is provided in the table below. The table lists the roles, skill sets of

personnel required for the above deliverables. The Bidder may respond with additional resources apart from the minimum required based on its assessment of the scope of work, deliverables and SLA

.

Sr No	Role	Qualifications and Experience	Minimum No of resources	Level
1	Lead/Sr. Security Analyst/ Sr. Technology Specialist	Education: B.E. / B. Tech / MCA or equivalent degree. Desired Certification: EC Council-CEH/Comptia Security+/CISSP/CHFI, OEM certifications. 5+ years of relevant experience in managing all aspects of risk and incident analysis in SOC. Must have experience in managing at least 1 projects for enterprise scale Clients. · Shall be responsible for deployment, maintaining, tuning, monitor and managing all aspects of client SOC. Responsible for coordinating, in a timely manner, all activities necessary for security incident monitoring, analysing incidents / risks, incident / risk containment, identifying root cause, initiate problem resolution, incident / risk response and communication.	1x(L3) and 2xL2	L2, L3
2	Security Analyst	B.E/B. Tech/ MCA degree · Certified with: OEM Certification/ Certified SOC Analyst (CSA)-EC Council/ CompTIA CySA+· 3+ years of overall experience with at least 1 years of relevant experience in all aspects of Incident monitoring in SOC	5	L1

10.2 **General Guidelines:**

10.2.1 The SOC team will work in 24x7x365 environment and personnel resources should be able to work in shifts and flexible working hours to support the operations.

10.2.2 BMRCL reserves the right to interview all the personnel resources to be deployed on the project and reject if not found suitable for the project.

10.2.3 At a later stage also if any of the personnel resources are found unsuitable to perform duties or any of the personnel resources violates any of the BMRCL guidelines, BMRCL may seek removal of all such personnel resources.

10.2.4 BMRCL expects to build a strong team and there should be no single point of dependency on any one individual. BMRCL's services should always remain immune to any such dependencies.

10.2.5 Bidder is required to obtain permission from BMRCL in writing before removing any of the personnel resources from the project.

10.2.6 BMRCL expects deployed resource / personnel resources to constantly keep upgrading their product / domain knowledge & skills.

10.2.7 As soon as BMRCL adopts a newer version of an existing technology, BMRCL expects the existing staff working in the project to get certified on the same or the Bidder should arrange for the additional resources with requisite qualifications/certifications.

10.2.8 Proper on-boarding and off-boarding processes are required to be followed.

10.2.9 All the staff are required to abide by the BMRCL's applicable policies and NDA.

10.2.10 The teams should be adequate to ensure the unhindered 24x7x365 operations and support.

10.2.11 L3 Engineer /Team Lead would be the single point of contact for BMRCL.

10.2.12 BMRCL should be provided with a dedicated and exclusive team.

10.2.13 A detailed shift roster must be published at the start of the month in consultation with BMRCL

10.2.14 The bidder should factor in an increase of 15% on personnel resources on YoY basis at the agreed cost and Terms & Conditions in this Tender However, BMRCL will take a final call on this at its own discretion.

10.2.15 The onsite resources must work as per BMRCL's working days and hours or as decided by BMRCL for smooth functioning of BMRCL SOC.

10.2.16 Bidder will be responsible for police verification & background checks of all resources before on boarding.

Minimum Roles and Responsibilities:

Resource Level	**Roles & Responsibilities**
L1(Security Analyst)	Level 1 analyst will identify, categorize, prioritize, and investigate events rapidly utilizing triage and response guidelines for the enterprise using commonly available SOC log sources that include: • Firewalls and network devices. • Infrastructure server and end-user systems. • Threat intelligence platforms. • Web proxies. • Application logs and web-application firewalls. • Identity and access management systems. • Cloudand hybrid-IT provisioning, cess,and infrastructure systems. • Antivirus systems. • Intrusion detection and prevention systems. Monitor incoming event queues for potential security incidents. Perform initial investigation and triage of potential incidents and escalate or close events as applicable. Monitor SOC ticket (or email) queue for potential event reporting from outside entities and individual users. Maintain SOC shift logs with relevant activity from the shift. Document investigation results, ensuring relevant details are reported to level 2 analyst for final event analysis. Update or refer SOC collaboration tool as necessary for changes to SOC process and procedure as well as ingest SOC daily intelligence reports and previous shift logs. Conduct security research and intelligence gathering on emerging threats and exploits. Perform additional auxiliary responsibilities as outlined in the console monitoring procedure. Communicating emergency alerts & warnings to designated stakeholder/ departments/ SOC.
L2(Sr. Security Analyst)	Monitor SOC Solution Console & Dashboards and provide response to the reported incidents Filtered by L1. Monitor and review the L1 activities Support the day-to-day operation of a highly available distributed multi-clustered multi-tenant SOC Solution deployment. Perform initial analysis for known issues and provide the appropriate recommendations for closure. Monitor & Reporting of system components health and take necessary action in case of any observed issue. Provide notification and communication with Incident management and respective application team upon threat detection. Perform analysis on the reported incidents, determine the root cause, recommend the appropriate solution.

	Should provide real time situational awareness to the BMRCL's stakeholders. Use and apply learnings from incident and provide recommendation for standardizing the SOC Solution. Develop and implement processes for interfacing with operational teams and other supporting teams. Ensure the SOC Solution integration is intact among the BMRCL SOC solutions, other assets Design, create and customize the dashboards as per the BMRCL's requirements. ensure the necessary BMRCL SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas. Automating Day to Day Tasks related with SOC Solution Operations (but not limited to) Above is illustrative list of general activities. All Technology specific activities Related to SOC Solution to be carried out. SOC Solution Management, SOC Solution Monitoring, SOC Solution Operations, SOC Solution Automation, Content Development to fine-tune existing rules & develop new content based on latest threat vectors. Ensure & keep improving SOC Solution platform for better Return on Investment. Should have good understanding on MITRE attack framework.
L3(Sr. Technology Specialist)	Monitor and review the L2 activities Should provide real time situational awareness to the BMRCL's stakeholders. Use and apply learnings from incident and provide recommendation for standardizing the SOC Solution. Ensure the SOC Solution integration is intact among the BMRCL SOC solutions, other assets Design, create and customize the dashboards as per the BMRCL's requirements. Ensure the necessary BMRCL SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas. Support on boarding and maintenance of a wide variety of data sources to include various OS, appliance, and application logs. Create Custom queries, custom dashboards, and visualizations to support BMRCL's requirements and monitoring of the SOC Solution deployment Create and manage SOC Solution knowledge objects to include apps, dashboards, saved and scheduled searches and alerts Support access requests and modifications and permissions Support troubleshooting and remediation of issues as they arise with data ingestion and SOC Solution infrastructure Work on Improvement of overall posture of SOC Solution deployment to achieve best return on investment. Review SOC architecture and suggest any updates Monitor & report on cyber threats and suggest any changes needed to protect the organization in SOC Solution, Leading End-to-End Implementation of the suggested changes along with L2. SOC Solution Management, SOC Solution Monitoring, SOC Solution Operations, SOC Solution Automation, Content Development to fine-tune existing rules & develop new content based on latest threat vectors. Ensure & keep improving SOC Solution platform for better Return on investment. Should have a very good understanding on MITRE attack framework. Recommend SOAR workflows.

11. SOC Tools, Equipment's, Platform

11.1 Mentioned below are the requirements of the SOC that the vendor should comply with. Please explain the compliance in the remark's column and with reference to relevant sections in the proposal.

11.2 Following SOC tools must be configured for 99.9% Availability calculated on Quarterly places

- On-prem security platform
- SIEM
- SOAR
- SOC
- UEBA
- NOC

Sl. No	Technical Requirements - SIEM	Compliance (Y/N)
1	Proposed solution must be platform supporting Visibility, detection, investigation, and response	
2	Next Gen Platform must enable BMRCL to:	
	-Gain complete visibility into security data from a single pane	
	- Reduce events into a prioritized list of the most important alerts	
	- Leverage AI ML models with automated, advanced analytics and threat intelligence to speed investigation time	
	- Scale rapidly with out of the box use cases and integrations	
	- Drive compliance and manage regulatory risk	
3	Must Support a wide variety of technologies, applications, and	
	cloud services to help customers gain comprehensive visibility into enterprise-wide activity	
4	The solution Should include pre-built Device Support Modules, Solution must be capable of simple ingesting data from number and variety of log sources	
5	Solution Must intelligently correlates and analyses a variety of data types	
	from a wide range of sources, including the following:	
	— Endpoint data: from the Windows event log, Sysmon, nmon , EDR solutions and more	
	— Network activity data: from firewalls, gateways, routers, switches or sensors,	
	— Vulnerability data: From antivirus tools, vulnerability scanners, intrusion detection systems, intrusion prevention systems, data loss prevention systems and more	
	— Cloud activity: From SaaS and IaaS environments, such as Office365, SalesForce.com, Amazon Web Services (AWS), Microsoft Azure and Google Cloud	
	— User and identity data, Access permissions and groups : Ingested from Active Directory, LDAP, or other identity and access management solutions	
	— Application data: From enterprise resource planning (ERP) & COTS or Any other custom / in house application	
	solutions, application databases, SaaS applications, Mail solution and more	
	— Threat intelligence: From third-party & Open-Source threat intelligence feeds	
	— Container activity data: from container management	
6	Next gen Platform must include Security Big Data Lake/Central repository for security data, Security Analytics, Log Forensics, Ingestion from variety of sources including Applications, OT, IT, Network and Security with support for open choice of big data solution for future use	

7	SIEM solution must apply intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions using Agentic AI and GEN AI	
8	The proposed solution should be sized for sustained data of 5,000 EPS or equivalent Gb/day or equivalent CPU - capacity based at all layers but should be able to handle peak of 10,000 EPS or equivalent GB/day or equivalent CPU - capacity based at all layers without dropping events or queuing events and must take burst of 50000 EPS or equivalent GB/Day. There should be no limitation on the number of servers, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users, or data source count changes, till the time data ingestion size remains as per ask	
9	Proposed solution must be enterprise horizontally scalable solution with Mircoservices Architecture , adavnced Analytics and predictive capabilities.	
10	Data Ingestion should be fast and OEM solution must be capable of ingesting data from all IP sources also including Applications both home grown and commercial off the Shelf applications. In case of parsing requirement for any customised device or applications, it must be owned by OEM to provide same in 7 days free of cost, so that organization should not get non-compliant or should have any threats unidentified.	
11	In case of any version change or version upgrade of devices, OEM must ensure data ingestion should not stop and there should not be any data loss and should be done with no/minimal downtime	
12	The Proposed solution should have capability to collect logs real time from most of the standard platforms like Microsoft Windows, Linux (All flavours), MAC OS,AIX, Solaris, Firewalls, Network, other security devices or solution, identified database servers, endpoint security management servers, web application firewalls, network firewalls ,Active Directory servers, Web servers, private cloud etc. Solution must support historical data imports in any data formats with no extra cost or EPS and should be able to build correlation using the same	
13	The Proposed solution should have inbuilt security mechanism for protecting itself from security attacks	
14	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc (High availability)	
15	The proposed solution must support caching mode of transfer for data collection, so as to ensure data is being logged in the event loss of network connectivity, and resume sending of data upon network connection.	
16	The proposed solution must be able to collect data from new devices added into the environment, without disruption to the ongoing data collection.	
17	The proposed solution must provide for secure user access via HTTPS, ssh.	
18	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click.	
19	The Proposed solution must offer all the below built-in threat detection techniques out of the box: 1. Detect Web Application Threats. 2.Detect APT Threats.	
	3.Integrate with leading HoneyPot solutions. 4.Integrate with leading NBAD, NDR tools. 5.Give visibility of endpoints also by integrating with EDR, DLP, HIPS, Antivirus etc for endpoint analytics. 6.Integrate with SOAR tools for automation. 7.Integrate with leading Threat intelligence Platform (TIP).	

20	The proposed solution must provide a query interface that allows users to search for data stored within the solution. it should provide view and api mechanism to run any custom query	
21	The solution shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension with inbuilt data optimizer to optimize data while data collection itself	
22	The solution should be able to part and filter logs based on type of logs, date etc.	
23	The proposed solution should be able to receive, ingest and index structured or unstructured data and no events should be dropped	
24	The solution must have an incident review framework for incident management. Incident review framework to facilitate incident tracking, investigation, pivoting and closure, with self feedback mechanism for marking true/false positive/finetuning	
26	The proposed solution must be able to read data input from the following static log file formats:	
	a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)	
	b. Windows Events Logs	
	c. Standard Log Files from applications such as Web (HTTP/HTTPS) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.	
27	The solution must be able to provide the capability to fully customise alerts, reports, and dashboards to the business requirements from Application UI	
28	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc to provides rapid insights and operational visibility into large-scale Unix and Linux environments machine data: syslog, metrics from log data.	
29	Solution must be capable of providing real time and on demand access to data sources such as evolving format, Custom API's, interfaced incl. text, XML, JSON, Data Base connections, Network Ports, Connections or from log data., and files	
30	The solution must be able to provide the capability to annotate events, modify status, build a chronological timeline for the incident before and after a triggered event.	
31	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.	
32	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or reindexing so that complex report or user defined reports can be built.	
33	The solution must be able to support the following indicators:	
	- Network, IP	
	- HTTP Referrer, User Agent, Cookie, Header, Data, URL	
	- Domain	
	- Endpoint	
	- File Hash, Name, Extension, Path and Size	
	- Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data	
	- Process Name, Arguments, Handle Name, Handle Type	
	- Service Name, Description	
	- Certificate	
	- Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm	
	- Email	

	- Email Address, Subject Body	
34	Solution should support machine learning auto triaging & manual triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, AV, EDR, Firewall (all with Well Known OEM's as well as Open source platforms).	
	Solution should support AI and machine learning driven triaging algorithms that considers contextual parameters, historical behaviour, and external threat intelligence to enrich and arrive at a triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same	
	· Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert.	
	· Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on.	
	· Central Threat Intelligence feed should also be applied to identify threats through known bad actors	
35	Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters . it should be configurable from UI without any restart of services	
36	Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise (IOCs), external network connections.	
37	The proposed solution must support real-time remote indexing of data sources to minimize the opportunity for alteration of audit trails on compromised hosts.	
38	Solution should support models to build up the entire attack chain from attack inception, progress of the attack and spread to attack in the network.	
39	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if	
40	Solution should support features to identify attacker attributes including threat intelligence score of attackers, who-is lookup information, geomapping in a single console.	
41	Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioural based use cases.	
	-Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time	
	-Using distance formula to detect geographically improbable access	
	-To measure the randomness of domain names that can be potentially from malware domain generated algorithms.	
42	Solution should support integration with any number of open source or commercial IOC sources available today or in future. List the supported sources which can be integrated with Solution and brief on the integration approach. Solution should support features to analyse and identify the impact of this attack on other assets.	
43	Solution should provide features to do free flow visual analysis of alerts and logs from integrated data sources based on custom criteria. This visual analytics feature should have appropriate graphical representation options to visualize large scale data.	
44	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability for security alert in Window Unix and Linux environment. to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment.	
45	The solution should have high availability feature built in for automated switch over to secondary collector/integrator in the event of primary collector failing. No performance degradation is permissible even in case of failure	
46	Solution should capability to filter undesired, non-security logs at collection, processing, and visualization layer	

47	The proposed solution must be able to read data input from the following static log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b. The solution must be able to accept the following live data streams from cloud server less functions like raw or JSON formatted data over HTTP/HTTPS.	
48	The proposed solution should be able to consume logs from any log source without writing parser beforehand or while integration. Parsers should be built once log is ingested (Note: there should not be any drop of events/data. Such events/data can be parsed once parser is ready)	
49	Solution should provide capability to search raw and indexed logs as full text, natural language, time range values, IPs, IP subnet mathematical & statistical functions, logical operators, occurrences count, regex, similar events, first & last seen, predictive & prescriptive search suggestions etc.	
50	Solution should be capable of retrieving the archived logs for reporting, analysis, correlation, investigation, and forensics.	
51	The report should be parameterized, and the user should be able to scale the parameter as needed and Out-of-box aging analysis of incident should be available. Solution should support dynamic reports scheduling and prioritization.	
52	The solution should provide detection/correlation of logs with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open-Source TI feeds)	
53	The solution should have a centralized correlation engine and a management center/console which allows creation of an unlimited number of correlation rules	
54	The solution should be able to perform different correlations (but not limited to): Rule based, Historical based, Heuristics based, Behavioural based, etc., across different devices and applications	
55	The solution should have the ability to correlate all the field present in a log/flow data.	
56	The solution should provide a web-based, user-friendly console or a wizard-based console to create rule.	
57	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix, and Linux environments machine data: syslog, metrics from log. and configuration files.	
58	The proposed solution should have the ability to perform free text search on events, incidents, rules, and other parameter	
59	The platform should provide the capability to use Machine Learning models on the data, peer groups, watchlists and multple risk profiles	
60	The data storage and indexing component should provide the ability to scale "horizontally", meaning the capability to start with a set of nodes within a single data store/cluster and keep adding additional nodes to handle larger volumes of data without having the need to replace or upgrade the existing nodes in the cluster.	
61	The solution should also be capable of collecting and indexing machine data from all the log sources including OS platforms, Middleware, Databases, network & security devices, applications etc., and allow for collecting, indexing, searching, monitoring, and analysing logs in real-time	
62	The solution should have an inbuilt parsing mechanism available in UI to be able to parse the logs obtained from multiple log sources (in the cloud and on-premises) including OS platforms, network & security devices, applications, IAM systems etc. and convert them into a standard log format on which the analysis can be done. Custom parsing shall also be available for custom applications, if out of the box parsing is not available.	
63	The solution should have the capability to add as many fields/columns in the index. The solution should support any number of fields in a particular row of data and should be able to store any amount of data in a particular field	
64	The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing url parameters to any third-party website. The Report should be scalable IP-wise,	

	device-wise, user-wise, data-wise, location-wise based on requirement between any two dates.	
65	The solution should have pre-defined rules for conducting intelligent analytics on real-time and historical log data obtained from multiple log sources (in the cloud and on-premises) including OS platforms, network & security devices, applications, IAM Systems etc. as well as threat feeds obtained from different sources	
66	The proposed solution should have AI ML capabilities.	
67	The solution should offer the flexibility to develop customized correlation rules for conducting intelligent analytics on real-time and historical log data obtained from multiple log sources on multiple parameters (like Hosts, Geographies, recurring activities) including OS platforms, network & security devices, applications etc. as well as threat feeds obtained from different sources	
68	The solution should have capability of conducting detailed analytics, business intelligence analytics, machine learning, pattern analysis, trends & spikes, anomaly detection, access outlier analytics, VAPT Analyitcs and Patching Prioritization etc	
69	The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE/CIS/NIST/ Kill Chain etc)	
70	The solution should have capability of conducting search across real-time and historical data as and when required with no limitation on date range	
71	The proposed solution must provide the following capabilities as a Security Analytics Platform:	
	a. One single syntax that can be used universally for search queries, alerts, reports, or dashboards, SIEM, SBDL.	
	b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure	
	c. Risk management technique to apply individual risk scores to any asset or user based on relative importance or value to the business.	
	d. Threat intelligence technique that automatically collect, aggregate, deduplicate indicators of compromise from threat feeds	
72	The solution should have monitoring and alerting capabilities for individual and correlated real-time events	
73	The solution must detect and alert on following:	
	- Firewall port scans	
	- Brute force attack	
	- Network intrusions or suspect traffic	
	- Backdoors and Trojans connections	
	- Connect to/from bad/blocked URLs - Analyse web proxy data for connections to malicious URLs	
	- Emerging Threats	
	- Detect and update on emerging threats	
	- Notify security incidents via Voice/Portal/Email	
	- Daily/Monthly report on security monitoring service	
	- Alert in case unavailability of event logs from registered device	
	- TOR, DNS tunnelling kind of malicious communications	
	- DNS query for malicious domains.	
	- Detect suspicious object that are embedded within files through malicious	
	PowerShell scripts for opening a command shell	
74	Solution must provide capability of Log Filtering all logs are not needed for the compliance requirements faced by organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.	

75	The solution should provide a pluggable framework to make use of APIs. The framework should support ingestion of data from other applications, export of data from the solution using APIs as well as orchestration of triggers. This solution should provide the ability to use this capability to integrate with other applications for automating tasks and workflows.	
76	The proposed solution should provide end-to end capability to setup an Analytics Platform for storage, indexing, searching, analysis, correlation, reporting, visualization, orchestration of different types of structured / semi structured data generated within the organization.	
77	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics, and performance data for industry relevant formats so that the analyst can have end to end visibility of the ecosystem.	
78	The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies, and outliers across all the data etc. into a single dashboard available from log data.	
79	The proposed solution must possess built-in/integrated feature for anomaly detection:	
	a. Uses historical data as a baseline to forecast future patterns, thresholds, and tolerances	
80	Dynamic, intuitive, parameterized, and customizable dashboards should empower personnel resources in the SOC to take prudent decisions. Multidimensional, analytical, trend &pattern-based dashboards should be recommended by individual technology based on their own self-learning capability.	
81	Solution should have end to end security mechanism to ensure security of logs, data, information, alerts, users, configurations etc. at rest / storage / database, during processing and in transit.	
82	Solution should have capability to receive, ingest, index structured, semi structured, unstructured data and transform, aggregate, and analyse structured data for security monitoring.	
83	Solution should be capable to monitor and notify whenever any asset integrated with it stops sending logs/ events / flows/ data / traffic /TI etc.,	
84	Solution should be able to provide raw and normalized logs/data storage as per the retention requirements for SIEM technology as outlined in the scope of work in this RFP	
85	Solution should be capable to correlate events, network activity data, alerts, and vulnerability data to provide complete view of security threats and generate real-time security alerts	
86	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition it should provide a summary of how the attack or detection technique maps to any of the following:	
	--ATT&CK MITRE, an adversary behaviour model that describes the actions an adversary might take.	
	--Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective.	
	--CIS Critical Security Controls	
	--Data types that are referenced within the rules/search and that need to be populate	
	--There should be template to upload advisories in an automated manner.	
	--There should be templates to design and trigger work flows automatically.	
	--Any other customizable templates as per department requirements.	
87	Solution should support multi-tenancy feature with segregation of data and display for different entities.	

88	Raw, normalized correlated logs shall be stored to the attached storage/SAN/NAS for the future reference and forensic activities in the event of incident.	
89	Solution must be able to store log data both locally and with SAN/NAS integration.	
90	The solution must store logs online for 90 days followed by near Offline storage for 3 years. It should support UI based data masking and unmasking , it should have RBAC control for Data view based on role	
91	Solution must be IPV6 ready.	
92	Solution shall provide real time threat intelligence from at least one commercial and one open-source feed	
93	Threat Intelligence Feed shall be included with the SIEM solution for Five (5) year warranty along CAMC period.	
94	Solution must retrofit with any legacy application/ devices/ equipment event sources, which may or may not be able to push logs. It shall be capable of collecting events from all Applications/ devices/ equipment event sources.	
95	Solution must be horizontally and vertically scalable to support increase in EPS/data	
96	Solution should support min 10 security analysts with unlimited actions from day one and provide Role Based Access (RBAC) to differentiate between analysts and administrators for restricting access to investigations, Jobs, Scripts, playbooks and admin tasks	
97	The proposed solution should provide more than 90 percent compression on queryable data and should allow historical log exports of raw logs from big data solutions	
98	Solution should support multitenancy and provide a clear Architecture for function in multitenant environment. Tenant Creation and Adminstration should be included in the WEB Ui and should be done without any restarts not impacting other tenants. Each Tenant should be individually configurable for any licences / data pipelines / retention periods and analytics	
99	The solution should support an integrated MITRE Framework and provide an interface to visualize all the various correlation rules deployed in the SIEM and their mapping with the MITRE framework to evaluate whether all TTPs on the MITRE framework have been adequately covered with rules.	
100	The solution should be able to identify the common sources or targets across all the alerts raised historically and also identify how many alerts have been raised by these common sources or targets.	
101	The solution should also correlate the alerts and give a view of the entire threat campaign to the user for quicker analysis and reducing alert fatigue.	
102	Solution should support creation of customized reports in formats like csv, doc and pdf with custom logo of the organization.	
103	Solution should be able to integrate with security devices like Firewall, IPS, endpoint Security solution, APT solution, WAF etc. from day one. Solution should support integration with third party OEM products including but not limited to the following technologies:	
	a) Forensic tools,	
	b) IT (e.g. AD, SAML),	
	c) SIEM Solution,	
	d) Communication tools (e.g. Email),	
	e) Endpoint Security Solution,	
	f) Network Security Solution,	
	g) Threat Intelligence,	
	h) Dynamic malware analysis.	
104	Solution should support Dashboard and any Dashboard which can be provide high level view of Platforms KPI's to the BMRCL.Dashboard should be exportable, RBAC controlled and should have facility to email dashboards periodically	

105	The solution should be sized to store the historical incident data related to alerts, incident cases etc. for the minimum period of 5 years	
106	The bidder shall propose hardware sizing such that at any point in time during the contract period, CPU, memory utilization should not exceed 70% and storage space utilization should not exceed 70%. In case the server resource utilization exceeds 70% or storage space utilization exceeds 80% the additional/new hardware has to be provided by Bidder to optimize the performance within the indicated levels, at no further cost to the BMRCL.	
107	Proposed SIEM solution should have capabilities to be integrate with SOAR, EMS/NMS, ITSM etc.	
108	The solution should be able to access structured data in your logs without extraction	
109	As part of project deliverable the bidder must provision for Unlimited parser / integration development for new or updated log sources which will also need to be extended to soar action plugins as well as new dashboards and report on an ongoing basis as and when required as stipulated by regulators or as new technology addition keeps happening in the organizations environment. All of this also are required to be meeting the stipulated SLA of 96 hours	
110	SIEM should have User and Entity monitoring through behaviour analytics leveraging AI & ML models on premise	
111	The NGSIEM correlation engine should support the identification of “low and slow” attacks by providing capabilities of data mining historical incidents and generating on-screen patterns which can then be translated into correlation rules for future detection and analysis	
112	NG SIEM should support automated data parsing / mapping. NG SIEM should be able to create custom attributes on the fly . NG SIEM should have capability to store raw and processed logs, together, in the same data store	
113	NG SIEM should have dynamic peer groups creations to reduce false positive, NG SIEM should monitor orphan accounts, access collectors, access outliers, privileged access	
114	The Next Gen SIEM collection/Processing mechanism must provide inline options to reduce event data by filtering out unnecessary event data	
115	Next Gen SIEM should have an ability to convert search queries into threat models which can be executed on the real-time data and flag any high risk users / entities	
116	NGSIEM Should support Log ingestion from indifferent Logs sources in any format (ex: Badge access Data / Biometrics, Home grown applications)	
117	SIEM ,SOAR & UEBA every module that is proposed by bidder from same OEM stack , all modules should carry respective "Make in India" compliance certificate	
118	GEN AI : •The SIEM solution must have inbuilt/ integration with Generative AI platforms should support to responds to the Security Operations Center queries/prompts •The responses could be about platform reporting such as platform health, latest vulnerabilities, high severity incidents , most frequent incidents, top risky users and top risky devices based on the incidents & also suggestions on efficient operations to guide SOC operations	
119	Agentic AI : SIEM should have Agentic AI for -Agentic AI agents should run in parallel to accelerate query across big datasets -Faster Threat Detection, Investigation, Response and to lower SOC workloads to resolve L1 tasks autonomously , -Better accuracy using context-aware risk scoring -Dynamic SOAR playbooks for faster automation	

11.3 **SOAR**

S.No	SOAR & TIP Requirements	Compliance Yes/No
1	Solution should be able to deploy on-prem virtual machine or cloud-based with the same license.	
2	Solution should run the scripts/integration modules/action processors inside dockers & containers to protect the system from executing malicious scripts or harmful commands.	
3	The solution should support User authentication via LDAP and SAML, SSO, AD, etc.,	
4	Solution must be web based without the need for installing an additional client software for administration and routine day to day usage requirements.	
5	The solution should support Role-Based Access Control (RBAC) mechanism for incident and other related system data which defines the segregation of duties.	
6	Solution should support deployment for access remote networks which are behind the firewall or isolated from Internet	
7	Solution should support backup/restore and provision for creating a HOT backup/standby server.	
8	Solution should provide new content pack which includes new feature upgrades on a periodic basis free of charge.	
9	Solution should have provision for storing security incidents/alerts and related artefacts for minimum 36 Months. Data retention & data archival settings should be or configurable.	
10	The solution must have a web-based GUI for analysis, reporting and other management activities.	
11	For audit reasons, the solution must be capable of logging all failed attempts to login into the user console.	
12	Solution should support periodic reporting and compilation of evidence for audit requirements	
13	Solution should provide reporting/dashboard functionality to fetch security incident report based on incident category, incident status threat score, threat intelligence inputs, specific asset. specific agency, time duration, criticality/severity, creation date, closure date, etc.	
14	Solution should provide automated incident SLA breach report based on severity, type, creation time, closure time, response time, etc.	
15	Solution record audit trail of all manual and automated steps, actions during execution of a playbook.	
16	Solution should provide management summary dashboard with information like statistics about incidents, solution effectiveness in terms of cyber incidents handling times, etc.	
17	Solution should support creation of customized reports in formats like csv and pdf with custom logo of the organisation	
18	Solution should support creation of customized widgets based on the requirements. These widgets should then be allowed to add to dashboard and exportable in report in formats like csv and pdf with custom logo of the organisation	

19	Solution should have integration support for various network and security solutions not limited to Firewall, SIEM, IPS/IDS, EDR, ITSM and WAF.	
20	Solution should be capable of implementing a new integration without any coding requirment and should support no code based implementation.	
21	Solution should auto-assign a unique ID to every incident/case that has been ingested into the system	
22	Solution must provide UI based wizard to manually create incidents.	
23	Solution should support creating an incident/case based on an email input, XML, Manual entry, URL, An API Call, Ticketing system, Custom portal (WebForm), Syslog, free text, JSON etc.	
24	Solution should allow an analyst to upload file attachments as artifacts, evidence etc. / should not get deleted or modified once added	
25	The solution must provide central management of incidents and administrative functions from a single web-based user interface.	
26	Solution should track all forensic data related to an incident in one location (s system images, snapshots etc) and view the history of evidence across the entire incident	
27	Solution should support updating existing out of the box integration and allow addition of new tasks without any coding requirement.	
28	Solution should have capabilities to map the incident automatically as well as manually to MITRE ATT&CK navigator	
29	The solution should have capabilities to map the incident, attacker, TTP and software data to the MITRE ATT&CK navigator	
30	The solution should have capabilities to correlate between the Incident, IOC, TTP, malware family and Threat actor within the platform	
31	Solution should use playbooks/runbooks with an editor which supports visual creation of playbooks without the need to code by native integration to third party tools and processes	
32	Solution should have the ability to suggest malicious phishing emails based on machine learning.	
33	Solution should allow creating new playbooks to map out the CIRT (Computer Incident Response Team) processes. Provision for building min 100 custom playbooks should be factored within the solution and should be scalable upto 150 custom playbooks.	
34	Solution should support reuse of existing task, and should provide capability to use nested playbook (playbook inside another playbook) to enrich incidents or resolve incidents.	
35	Solution should support out of the box playbook mapped to all the MITRE Tactics	
36	Solution Should allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks	
37	Solution should allow a single playbook to have Automated and Manual Tasks within the same playbook	
38	Solution should allow a complete playbook to be run automatically or manually and list out any exceptions	

39	Solution should record all manual and automated entries during execution of a playbook	
40	Solution should allow addition of adhoc tasks within a playbook	
41	Solution should support running playbooks as scheduled tasks at pre defined time intervals	
42	Solution must support provision to pass parameters to upstream/downstream task within a playbook	
43	The solution must have a mechanism to save and maintain multiple versions for the playbooks	
44	The solution should allow for viewing all or selected playbook and provide option for restoring to an older version	
45	Solution should support sending notifications to other users on playbook failures.	
46	Solutiion should be able to embed custom code into playbooks using custom utils.	
47	Solution should support implementing custom util using python , these utils should be allowed to be tested against the alert data at the time of creation.	
48	Solution should allow including multiple custom utils in one utility and allow logging the information from multiple utils.	
49	Solution should allow automatic execution of playbook on the grouped cases and should allow automatic execution of playbook on the cases which are not grouped via the group rule	
50	Solution should be able to perform the enrichment using the integrated tools automatically for all the ingested alerts.	
51	Solution should support the tracking of the assets involved in one incident at a central place along with all the security control mapped the particular asset	
52	Solution should support the central tracking of all the assets involved within the incidents along with their current investigation status	
53	Solution should be able to map user/department/location/asset information to the incident	
54	The solution must be capable of securing and managing every type of asset such as servers, applications, endpoints, software and users related to the incidents being investigated.	
55	Solution should facilitate correlation of malicious campaigns by connecting the dots between incidents, vulnerabilities, threat actors, malware, and assets.	
56	Solution should be able to track the users involved in an incident along with providing details of the user present in the incident.	
57	Solution should be able to identify coverage gaps by identifying missing mandatory controls in the environment.	
58	Solution should have a feature of auto assignments of calls to analyst on the basis of complexity of case and availability of engineers in the shift	
59	Solution should allow scheduling of playbooks to allow execution at specific time along with scheduling of reports to be sent across recepients.	
60	Solution should allow running queries on the cases to fetch the cases depending on the analyst requirement.	

61	Solution should support various structured and unstructured Threat Intelligence feed formats gathered from a combination of Commercial, Open source, User-led, and Community-driven Intel sharing sources and also provide complete advisory of threats to enable the organization to plan countermeasures for taking proactive actions.	
62	Solution should support all the STIX objects out of the box and any feed ingested should be converted to STIX objects	
63	Solution should support open standard formats like CyboX, OpenIOC, Yara, STIX 1.0, STIX 2.0, MISP, XML, CSV, JSON, MAEC, IODEF etc.	
64	Solution should also be capable of supporting unstructured formats such as email, news, RSS Feeds, blogs, Free text etc. and should be capable of automatically normalizing it.	
65	Solution should have the ability to import and export Intel feeds in popular consumable formats such as XML, JSON, CSV, etc.	
66	Solution should be able to perform Normalization - Consolidating data across different sources formats.	
67	Solution should be able to do De-Duplication - Removal of duplicate information.	
68	Solution must provide additional information on IOCs, wherever requested, by integrating with WHOIS, Virus total, Shodan, Hybrid Analysis etc.	
69	Solution should support scoring of feeds or IOC to ensure only relevant feeds are worked upon by the analyst.	
70	Solution must be capable of ingesting vulnerability data from various sources to correlate during the incident investigation	
71	Solution should support automated indicator deprecation, in which the indicator gets expired after the decided time-span. The platform should also have an option to auto unblock IOC on deprecation.	
72	Solution should allow the analyst to mark the severity and risk, track and add comment/notes for the indicators.	
73	Solution should support interactive analysis with help of notes/ comments which can be shared with other analysts.	
74	Solution must support Threat Intelligence sharing format/protocols such as STIX/TAXII.	
75	Solution should record timestamp for all actions taken in an incident.	
76	Solution should have an incident analysis structured process to identify the source and the cause of incidents, analyse the extent of compromise for quick containment and minimize losses.	
77	Solution must be able to correlate an existing incident with a historical one if there is a match	
78	Solution should perfomr parsing all the SIEM message fields, including but not limited to: creation time; update time; source/dest IP; source country; category; system; rule-name; severity; dest IP	
79	Solution should be able to whitelist/blacklist IOCs on the platform and track the IOCs depending on the IOCs mentioned in the whitelist/blacklist.	
80	Solution must capable of publishing its own health reports for administration and maintenance	

81	Solution should have an option to configure and manage the SOC shifts within the platform	
82	Solution should support customizable dashboards for different roles and access levels.	
83	The service scope for initial deployment should include integration with out of box products as well as to build custom integrations(5) along with customization of reports/ dashboards/ queries etc.	

11.4 UEBA

Sl No.	UEBA Feature Requirements	UEBA Compliance (Yes/No)
1	UEBA should be based on unsupervised machine learning / deep learning so that it does not require any human/analyst to create data science models.	
2	UEBA should have all the behavioral detection models OOTB without any need of a data scientist	
3	The proposed UEBA should natively have ML/deep learning capabilities and should not have separate engine/compute requirements for running ML models.	
4	The UEBA must be able to monitor all the users in the organization. UEBA should not have separate data repository and should consume and operate on data lake or SIEM data repository. Use Case: Every single user can be source or a target of threat hence it's very important to cover all the users with UEBA solution.	
5	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning/deep learning and other statistical analysis techniques.	
6	UEBA should support user and entity-based behavior Analytics, it should provide MITRE ATT&CK framework intelligence on the generated on the models more than 85% coverage	
7	To be able to correlate across user access logs, network flow traffic and endpoint activities and apply data science models to detect those abnormal user and entity behaviors occur anywhere in the network	
8	UEBA should be an integral component as part of NG-SIEM and should have same UI as the NG-SIEM to provide event level and historical level analysis along with behavioral analysis and should be 100% on-premise without connecting to any internet based ML analytical engine. All ML/AI analytics should be done completely on-prem.	

9	Indicators falling under following high-level threat categories must be detected across endpoints, network flow traffic and user activities not limited to: · User Logins to Multiple AD Sites · User Login to Abnormal Host · User Logged into Multiple Hosts · Snooping User · Sensitive User Status Changes · Registry Run Keys & Start Folder · PowerShell & Scripting · Non-Standard Hours · Multiple Logons by User · Multiple Failed Logons · Mass Permission Changes · Mass File Rename · Mass Changes to Groups · Elevated Privileges Granted · Discovery & Reconnaissance · Data Exfiltration · Credential Dumping · Admin Password Change · Abnormal File Access · Abnormal AD Changes · Phishing · Data Exfiltration	
10	UEBA solution Should have open analytics where customer can create their own custom models using below ML templates	
11	UEBA solution Should be able to provide configurable analytical attributes for ML Models	
12	UEBA should present any user profile with 360 degree view of activities, alert stiching, risk profile, peer groups, devices, locations	
13	UEBA should present any entity profile with 360 degree view of activities, alert stiching, risk profile, peer groups, devices, locations	
14	UEBA should have ability for flexible entity creation and it should be based on real time	
15	UEBA should have a dynamic risk scoring based on AI / ML and should provide context	
16	UEBA should provide risk distribution based on outliers and analytics	
17	UEBA should have automated and configurable risk decay functions	
18	Machine learning/Deep Learning should be embedded across the platform (SIEM, SBDL & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	
19	UEBA should Provide an aggregated analytics UI dashboard to security analysts with ability for detailed drilldown investigation of specific events.	
20	UEBA should be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.	
21	UEBA should support Machine Learning (ML)/Deep Learning driven risk scores and risk profiles for user.	
22	UEBA should be a pure machine learning engine with no need to configure any settings not limited to baselines, thresholds, decays, risks scores. Also, there should not be any need to configure thresholds through settings during learning or production phase	

23	Proposed UEBA should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA specific fields	
24	Behavioral analysis UEBA should have embedded machine learning engine and there should be no separate app/plugin for same it should be natively	
25	The User and Entity Behavior Analytics UEBA must be integrated with SIEM, and leverages available Logs, endpoint (EDR) data for its behavior analytics.	
26	The proposed UEBA must be able to handle peak load for logs of 25000 EPS anytime from the day one without dropping or queuing of logs across all layers and there should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	
27	Proposed UEBA should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA specific fields.	
28	The UEBA must be able to monitor all the users in the organization. UEBA should not have separate data repository and should consume and operate on data lake or SIEM data repository.	
29	ML & AI based UEBA should be part of the same NextGen-SIEM and should support horizontal scaling of all components	
30	UEBA must have ability to configure rolling window of period for behaviour profiling	
31	UEBA must have ability to derive dynamic peer groups and perform behaviour analysis	
32	UEBA must have ability to import and execute custom behaviour models developed using standard technologies like java, python, etc.	
33	UEBA must have ability to build custom behaviour models without requiring any development effort and any upgrades	
34	UEBA must have ability to support fine-tuning of various meta-data attributes of behaviour models	
35	The UEBA should have in built feature to handle less false positives and it should fine-tune itself to change the behaviour baseline as per its new learning to help generate True positive events and Alerts The UEBA Solution must have ability to provide feedback on the UEBA results and retrain the models & customize the Risk score for each model if required The UEBA Solution must have abiltity to provide higher rate of True positive events and should eliminate manual investigation cycle as much as possible	
36	The UEBA must offer addition & development of custom machine learning models and upload of new external machine learning models through its console.	
37	The UEBA must use supervised and unsupervised machine learning algorithms	
38	The UEBA should not store data in proprietory index format and the normalized Data should be exposed to other Security Systems and applications to be used for collaborative Analytics if required	
39	The UEBA should support Machine Learning (Behaviour /Risk Profiling) as well as Static Rules based monitoring	
40	UEBA should be part of the same license, including the pretrained 4000+ ML Models and Secuirty analytics of the NG-SIEM license.	
41	UEBA must have natively built in SOAR and playbook automation.	
42	The UEBA must provide open choice of Big Data technologies including Hadoop, Cloudera, Hortonworks, Hbase, Crate, etc. and must be big data lake agnostic.	

43	UEBA should provide comprehensive Application and Audit Logs and offer protection for Log Tampering	
44	UEBA should support both - on premise and Cloud deployments	
45	UEBA should support collection of Logs and Data without the need of installation of Clients on Endpoints or Network Devices (clientless in nature)	
46	UEBA should support Deployment, Integration and Log collection with minimal or possibly no disruption to the Network / Services	
47	UEBA should provide Access Analytics and Identity Access Intelligence out of the Box	
48	UEBA should provide functionalities of Access clean-up , Activities on Rouge and Dormant account, Suspicious Account Activities	
49	UEBA should be able to Integrate with other NGSOC components i.e. SIEM, SOAR, TIP, NBAD and EDR platform	
50	UEBA should provide a "Single-pane-of-glass" view into high risk user / entity showing behavior pattern with respect to activities, locations, devices, sessions, usage and risk trends	
51	UEBA should have an ability to send alerts through email	
52	UEBA must support a Data Masking capability to remove sensitive data from the view of analysts, such as Government ID, passport numbers, social security numbers, credit card numbers, etc.	
53	UEBA should provide CASB / DLP Intelligence out of the Box	
54	UEBA should provide Privilege Access Intelligence out of the Box	
55	UEBA must Cluster Deployment for the big data lake nodes and have a multi tier storage in the Datalake like 30-90 and 365 days tiers for Hot, warm and cold tiers respectively	
56	UEBA must use supervised and unsupervised machine learning algorithms for any kind of data set	
57	UEBA should have in built feature to generate Less False positives and it should fine-tune itself to change the behavior baseline as per its new learning to help generate True positive events and Alerts	
58	UEBA should provide supervised and unsupervised machine learning algorithms by default.	
59	UEBA should Use machine learning algorithms for security analytics (atleast 3500 models) which should be all Trained models by the platfrom vendor.	
60	The UEBA platform should have a fully integrated Generative and Agentic AI assistant as a part of the platform at no additional cost.	
61	The UEBA should provide Rule Engine and a Machine Learning Engine which can facilitate writing of Rules and Models in graphical GUI Module (easy to use) and should support of ML models which are developed in house.	
62	The UEBA should record an audit trail of all manual and automated steps and actions during the execution of a playbook.	
63	UEBA must support the English/Multi Language on the Dashboards	
64	UEBA should have an ability to add/remove widgets depending on the investigation requirements	
65	UEBA must have Security and Compliance out-of-the-box.	
66	UEBA should have an ability to highlight top risks in a dashboard and an easy way to drill-down to anomalous events and raw data for further investigation	
67	The UEBA dashboards should support different views relevant to different stakeholders including top management, the operations team, Information Security Department.	

68	UEBA should have an ability to export only required columns from the Analysis Dashboard as part of Reports	
69	UEBA should support for creating personalized Dashboards depending on User Roles (SOC Analyst, Auditor, etc…) and have capabilities to share Dashbaords / Queries among specific Roles & User to facilitate collaboration over Security Analytics	
70	UEBA must support data obfuscation techniques to comply with privacy policies	
71	UEBA must have a data optimization capability built in to collect, stream, optimize and fork the meta data collected.	
72	Any failures of the UEBA event collection infrastructure must be detected and duly notify the specific email/mobile.	
73	UEBA must support both Agent and agentless mechanisms to get the Logs from Windows and Linux Machines.	
74	UEBA must have Real-Time Network Traffic Analytics natively with Netflows	
75	UEBA should be able to ingest any number of Third party Threat Feeds and Threat Intel Platform (natively or using API)	
76	UEBA integration with enterprise authentication / SSO platform for simplifies access	
77	UEBA must support 3rd party FIM integrations.	
78	UEBA should have an ability to export search results as reports or publish it as data visualization component	
79	UEBA must have ability Intelligent search providing auto-complete, auto-suggest capabilities based on contextual data	
80	UEBA should not store data in proprietary index format and the normalized Data should be exposed to other Security Systems and applications to be used for collaborative Analytics if required	
81	UEBA should support pivoting of search results based on various data elements including identity, entity, AD Attributes, HR attributes, resource, event, threat, etc.	
82	UEBA should support Machine Learning (Behavior /Risk Profiling) as well as Static Rules based monitoring for all users and entities and network elements	
83	UEBA must have multi-tenancy & RBAC to support MSP/MSSP . The Central Dashboard should be out of the box and inbuilt free of cost.	
84	The UEBA collection/Processing mechanism must provide inline options to reduce event data by filtering out unnecessary event data.	
85	UEBA should have an ability to grant permissions on a granular basis for different stakeholders' administrators, analysts, management, etc.	
86	UEBA should have an ability to support role-based access control (RBAC) to application functionalities and data elements	
87	UEBA should have an ability to create custom reports and schedule the same	
88	UEBA should have an ability to leverage AD groups to control RBAC	
89	UEBA should have an ability to schedule reports with periodic intervals & Reports can be delivered as CSV, Email, PDF	
90	UEBA should have an availability of out of the box reports for administration and management	
91	UEBA should have an availability of out of the box reports for analysts to make investigation decisions	
92	UEBA should have an availability of out of the box reports for audit and compliance	

93	UEBA should have an ability to convert search queries into threat models which can be executed on the real-time data and flag any high risk users / entities	
94	UEBA should be able to provide Basic Threat Detection for Rogue IP / Domains out of the Box using the Common Threat Feeds	
95	UEBA should have an ability for analysts and administrators to input internally developed indicators for detection and alerting.	
96	UEBA must have IOC Integration from Threat Intel from same Vendor's threat research labs on a daily basis.	
97	UEBA platform should have monitoring for Activity Ingestion Parse Failure Ingestion Deviation Perecentage Model Execution Data Correlation Big Data Storage Daily Big Data Storage Failed Job	
98	UEBA license shall not restrict the number of users and it should be bundled as a single license with the NGSIEM, without any cap on number of users or entities to be monitored	
99	UEBA OEM should have a registered office in India and should be supported by OEM's direct and own 24x7 support center based within the country in India.	

11.5 NOC

S/N	NOC Technical Requirements	Compliance (Y/N/)
1	24/7 Monitoring and Support: Continuous monitoring and support to ensure the network operates smoothly at all times.	
2	Incident Management: Processes for detecting, managing, and resolving network incidents swiftly to minimize impact.	
3	Network Performance Monitoring: Tools and techniques to measure and maintain optimal network performance and throughput.	
4	Security Management: Implementation of security protocols to protect the network from threats and unauthorized access.	
5	Event Correlation and Analysis: Techniques to correlate and analyze network events to identify patterns and prevent issues.	
6	Performance Reporting: Regular reports on network performance metrics to help with analysis and decision-making.	
7	Capacity Planning: Strategies to ensure network resources are sufficient to meet future demands and growth.	
8	Change Management: Procedures to manage and track changes in the network environment to avoid disruptions.	
9	User Support: Support services to assist users with network-related issues and ensure a positive user experience.	
10	Scalability: Ability to expand the network's capacity and functionality to handle increased demands smoothly.	
11	Multi-Dimensional Data Model: Data model that allows for comprehensive analysis across multiple dimensions for deeper insights.	

12	Powerful Query Language (PromQL): Advanced query language for effective network data interrogation and retrieval.	
13	Time Series Data Collection: Collection of time-stamped data to monitor and analyze network performance over time.	
14	Self-Contained System: Integrated system with all necessary components to operate independently.	
15	Service Discovery: Mechanisms to automatically detect and connect network services for seamless operation.	
16	Alerting: Notification systems to alert administrators about network issues or anomalies in real-time.	
17	Data Visualization: Graphical representation of network data for easier interpretation and decision-making.	
18	Efficient Storage Solutions: Storage systems designed to save data efficiently while allowing for easy retrieval and analysis.	
19	Pull Data Collection Model: Model where data is pulled from sources rather than pushed, enhancing control and efficiency.	
20	Extensibility: Ability to extend the network's features and functionalities through additional components and integrations.	
21	Hierarchical and Modular Architecture: Structured approach to network design, allowing for modular additions and easy management.	
22	Interoperability: Ensuring the network can operate and integrate with different systems and technologies seamlessly.	
23	**Certified Resources-** Resources with certifications (CEH, CCIE, etc.) and OEM certifications (Bidder to provide certification details]	.

11.6 Workstation with dual monitor

Sl.No.	Parameters	Parameter and Minimum Specification	Compliance (Yes/No)
1	Processor	Minimum latest generation i7 or Higher	
2	Motherboard	OEM Motherboard	
3	RAM	Minimum 16 GB DDR4 RM expendable to 32 GB	
4	Graphics card	Minimum Graphics card with 4 GB video memory (non- shared)	
5	Monitor	Monitors of 24" TFT LED monitor, with Minimum 1920 x1080 resolution, Minimum input of 1xDP, 1x HDMI, 1xDVI, Energy star 5.0/BEE star certified	
6	HDD	Min. 1 TB SSD Drive	
7	Other Accessories	Line/Mic IN, Line- out/Spr Out (3.5 mm), Minimum 6 USB ports (out of that 2 in front), 104 keys minimum OEM keyboard, USB Optical OEM mouse,	
9	Operating System	64-bit pre-loaded OS with recovery disc	

11.7 Hardware, Tools, Resources Requirement

Bidder Need to submit the hardware sizing as below table along with Bid, BMRCL will provision the Hardware and any other Item like OS, DB licenses requirements, the bidder should clearly mention these details in sizing document.

S.No.	Application Name	Physical/VM	No. of Instance	vCPU per VM	Memory/ VM	OS Storage (GB)	External Storage (TB)	Total External Storage (TB)	Disk type for External Storage	OS Details	Database Software if any	HA Required?	Remarks

Section IV: Service Level Agreement (SLA), Penalties & Payment Terms

1.1. Implementation Timeline & Penalties:

S/N	Measurement	Target	Penalty for Delay
1	Kick-off meeting	2 weeks from issuance of LoI/ Award of Contract	Rs 50,000/week or part thereof. Delay Beyond 4 weeks, BMRCL may terminate the contract and Forfeit the PBG.
2	Supply of all Components (Hardware, Software, License, etc.)	T1 = T + 8 weeks	A penalty of 2% of the prescribed payment for the milestone per week or part thereof subject to maximum of 20% of the prescribed payment. Delay beyond T + 10 weeks BMRCL may terminate the contract and Forfeit the PBG
3	Installation and Commissioning of all Components (Hardware, Software, License, etc.)	T2 = T1 + 4 weeks	A penalty of 2% of the prescribed payment for the milestone per week or part thereof subject to maximum of 20% of the prescribed payment. Delay beyond T1 + 6 weeks BMRCL may terminate the contract and Forfeit the PBG
4	Final Acceptance Test (Go-Live of the Project)	T3 = T + 14 weeks	A penalty of 2% of the prescribed payment for the milestone per week or part thereof subject to maximum of 20% of the prescribed payment. Delay beyond T2 + 4 weeks BMRCL may terminate the contract and Forfeit the PBG
5	Deployment of manpower proposed for O&M of SOC	Within 15 days of Go-Live	Rs. 20,000/- per individual manpower / per week of delay. To be measured on pro-rata basis as per deployment of manpower. Delay beyond T3 + 3 weeks BMRCL may terminate the contract and Forfeit the PBG

T = Date of Award of Contract

1.2. Service Level Agreement & Penalties

1.2.1 The Successful Bidder is required to execute a Service Level Agreement with BMRCL covering all terms and conditions of this tender. Bidders need to strictly adhere to the Service Level Agreements (SLA). Services delivered by the bidder should comply with the SLA mentioned in the table below and the scope of services mentioned herein above. SLA will be reviewed on a quarterly basis.

Sl.No.	Service Area	Service Level
1.	SOC Monitoring & Log Analysis Services	• 24x7 event / log monitoring and correlation of the assets in Scope. • 24x7 monitoring of the Database Activity using a Database Activity monitoring tool which directly integrated with the SIEM solution. • 24x7 Monitoring & recording of Security events at all the ingress points. • Event alerts within 15 minutes of the event • Mitigation of security events / threats • Availability of relevant logs for last 3 months • Real time dashboard view • Monthly consolidated report by 5th of every month • Quarterly Reports • Standard / Exception reports
2.	Security Intelligence feed Services	• Validation of advisories within 12 hours of new global threats & vulnerabilities disclosures.
3.	Reports & Dashboard	• SOC should provide daily / weekly / monthly / quarterly reports for each of the services in a timely manner. • Dashboard should give online view of all devices monitored with their status
4.	Others	• Bidder should provide up-to-date contacts and Escalation matrix. • The Bidder should procure a reputed commercial tools / software's for SOC. • Availability of operation staff on 24/7 basis. • Rule-based Review of Firewalls

Sl. No.	Definition	Measurement Interval	SLA Target	Penalty terms
1.	Device uptime / Device availability	Monthly	>=99.90%	>=99.90% No Penalty
				>=98.00% and <99.90% 0.5% of QGR value
				>=95.00%; < 98.00% 1% of QGR value
				<95.00% 1% of QGR value for every percentage drop
2.	SOC application / Software availability	Monthly	>=99.90%	>=99.90% No penalty
				>=98.00%; <99.90% 0.5% of QGR value
				>=95.00%; < 98.00% 1% of QGR value
				<95.00% 1% of QGR value for every percentage drop
3.	Manpower availability	Monthly	100%	Resource replacement with equivalent skills and experience / with approval from department – no penalty.

			Attendance as per defined in RFP document.	Level 1 resource absent: Equal cost of the resource proposed by the bidder per day on pro rata basis.
				Level 2 resource absent: Double the cost proposed by the Bidder per day on pro rata basis.
				Level 3 resource absent: 0.1% of QGR Value.

1.2.1.Operational SLAs

SLA Definition	Metric	Severity	SLA	Measurement	Penalty
Incident Management	Incident Response Time	Level 4	15 minutes	Quarterly	Rs. 7000/hour for every hour of delay
		Level 3	30 minutes	Quarterly	Rs. 5000/hour for every hour of delay
		Level 2	3 hours	Quarterly	Rs. 2000/hour for every hour of
		Level 1	6 hours	Quarterly	Rs. 1000/hour for every hour of delay.
	Incident Resolution Time	Level 4	4 hours	Quarterly	2% of QGR value for every hour of delay.
		Level 3	8 hours	Quarterly	1% of QGR value for every hour of delay.
		Level 2	2 days	Quarterly	0.5 % of QGR value for every day of delay.
		Level 1	4 days	Quarterly	Rs. 10000/day for every day of delay.
Service Request Management	SOC Tool Rules Update	Emergency	4 Hrs	Quarterly	1% of QGR value for every hour of delay
		Normal	2 days	Quarterly	1% of QGR value for every day of delay
	Vulnerability Scan	Emergency	4 hrs	Quarterly	2% of QGR value for every hour of delay
		Normal	2 days	Quarterly	1% of QGR value for every day of delay
	SOC Operations Effectiveness Review		Once in 3 Months	Yearly	2% of QGR value for every delay
	SOC Architecture Review		Once in a year	Yearly	2% of QGR value for every delay

1.2.2.Supply, Installation, Commissioning

- All the items as mentioned in the BOM should be supplied, delivered, and commissioned within the mentioned timelines. Any delay would attract penalty.
- In case only some items of BOM are not as per timelines, then penalty would calculate on pro-rata basis item wise.
- The date of commissioning would be considered the date when a written communication would be sent by the bidder to BMRCL for Go-Live readiness.

Note: Root Cause should be identified for all incidents; if root cause is not identified then additional penalties will be levied.

The security breach will include but not limited to successful penetration of any Virus, Trojan, malwares, zero-day attacks, intrusion, Denial of Service Attacks, …etc., up to the Server level. In case of any compromise of data due to the Security Breach then double penalty will be levied.

2 Payments Schedule

Sl.No.	Activity	Payment (%)
Table 1: Schedule-I		
1	Delivery of all components (Software, Licenses, etc.) at BMRCL & Successful installation, Testing, Integration, Commissioning	80% of the sum total of schedule I of financial bid
2	Successful completion of training & Final Acceptance test of entire solution	20% of the sum total of schedule I of financial bid
Table 2: Schedule-II		
1	3 Years CAMC/warranty and Back-to-Back OEM support and operation costs including manpower for the entire Infrastructure	Will be divided and paid in 12 equal Quarterly Installments after the end of each quarter (3 months). Three years will start from the date of successfully completion of Go Live.

--- xxx ----

PAGE INTENTIONALLY LEFT BLANK

SECTION 8 – DRAWINGS

This Section is Not Used.

PAGE INTENTIONALLY LEFT BLANK

SECTION 9 : PROFORMA OF BANK GUARANTEES

PROFORMA – A : Form of Bank Guarantee for Tender Security / Earnest Money Deposit

PROFORMA – B : Form of Bank Guarantee For Performance of Contract

PROFORMA - A

FORM OF BANK GUARANTEE FOR TENDER SECURITY / EARNEST MONEY DEPOSIT

(Reference ITT clause 14)

(To be stamped in accordance with Stamp Act, if any, applicable for the issuing bank)

To,
Bangalore Metro Rail Corporation Limited (BMRCL)
3rd Floor BMTC Complex,
K.H. Road, Shanthinagar
Bengaluru- 560027.
Karnataka, INDIA.

1. **WHEREAS** _____ *[Name and Address of the Tenderer]* (hereinafter referred to as the "Bidder" or "Tenderer") has undertaken for submission of Tender in pursuance of Tender Notification No. _____ for _____ *[Name of the Works]* (hereinafter referred to as the "Bid" or "Tender").

2. **AND WHEREAS** it has been stipulated in the Tender issued by Bangalore Metro Rail Corporation Limited (BMRCL) (hereinafter referred to as the "Employer" or "BMRCL") that the Tenderer shall furnish to Employer an unconditional and irrevocable Bank Guarantee from an Indian Scheduled Bank (excluding Cooperative Bank) or from a Scheduled Foreign Bank as defined in Section 2(e) of RBI Act 1934 read with second schedule, for the sum specified herein below as Tender Security(EMD) for compliance of the obligations in accordance with the Tender conditions. In pursuance to this, M/s_____ has requested for issuance of the Bank Guarantee for the sum specified herein below as Tender security (EMD).

3. **AND WHEREAS** we _____ *[Name and full address of the Bank including Email address]* having registered office at _____ (hereinafter referred to as the "Bank"), which expression shall unless repugnant to the context or the meaning thereof, include its successors, administrators, executors, assignees, do hereby agree to give the Employer such a Bank Guarantee drawn and payable at Bengaluru _____ branch on behalf of the tenderer.

4. **NOW therefore**, the Bank hereby affirm that it is the guarantor and responsible to 'Employer' and their successors, on behalf of the 'Tenderer' up to a total sum of INR/Foreign Currency/ies _____ *[the amount of Guarantee to be specified in figure and words in the respective currency/ies as specified in the Tender document]*. Further, the Bank hereby unconditionally, irrevocably and without demur undertake to immediately pay, the Employer upon the Employer's first written demand and without cavil, or arguments any sum or sums within the limits of the sum specified in this Bank Guarantee as aforesaid without the Employer being required to prove or to show grounds or reasons for the demand, by depositing/crediting to the Current Account of the Employer, the sums specified herein.

5. This Bank Guarantee is encashable at the issuing Bank's designated branch in Bangalore, Karnataka, India as mentioned below:
Name of the Bank, Branch and contact details Address Telephone no: & Fax No: E-mail Address Branch Manager/s name & mobile No: Bank Zonal Office Address, Telephone No, Fax Number, E-mail Address: _____

OR

This e- Bank Guarantee shall be encashable at the issuing branch of the Bank through NeSL portal.

6. The Bank hereby confirms that the Bank is on the SFMS (Structural Finance Messaging System) platform and shall invariably send an advice of the Bank Guarantee to the designated Bank of the Employer as given below:

Sl. No.	Particulars	Details
i	Name of Beneficiary	Bangalore Metro Rail Corporation Limited
ii	Name of Bank	Bank of India
iii	Branch	Cantonment Branch, Bengaluru.
iv	Address of Branch	49, Jyothi Mahal, St. Mark's Road, Bangalore - 560001
v	Account No.	840420110000760
vi	IFSC Code:	BKID0008404

7. This Bank Guarantee shall be encashed at the demand of the Employer on or before the due date.

8. The Employer shall have full rights to encash this bank guarantee at any time during the validity period and the 'Tenderer' shall have no right or claim whatsoever in the matter of encashment of the Bank guarantee amount by the 'Employer'. The Bank will be fully responsible in terms of the guarantee and obligation, to make immediate payment to 'Employer', without the consent of the Tenderer and without referring the matter to the 'Tenderer'.

9. The Bank will deliver the money required by the 'Employer' immediately on demand without delay without reference to the 'Tenderer' and without the necessity of a previous notice or of judicial or administrative procedures and without it being necessary to prove to the Bank the liability or damages resulting from any defects or shortcomings or debts of the 'Tenderer'.

10. Courts at Bengaluru, Karnataka, India shall have exclusive jurisdiction for adjudicating the disputes arising out of the encashment of the Guarantee, and, the said Bank undertakes not to revoke this Guarantee during its currency, except with the previous consent of the 'Employer' in writing and agree that any change in the constitution of the Bank shall not discharge its liability hereunder.

11. This Bank Guarantee will not be discharged due to the change in the constitution of the 'Tenderer' or change in the constitution of the bank.

12. This Deed of guarantee is signed and executed by Shri/Smt _____ and Shri/Smt _____ who is/are authorized by the Bank for issuing the guarantee on its behalf and their ID No/s. and Email address/es being_____ & _____ and _____ & _____ respectively.

13. The Bank's liability under this Guarantee shall not exceed the amount of _____ *[Indian Rupees/Foreign Currency/ies to be specified in words and figures].*

14. This guarantee shall be valid till _____ *[Date to be mentioned]*.

15. The pendency of any dispute or arbitration or other proceedings shall not affect this guarantee in any manner.

16. It is hereby agreed that the liability of the Bank under this guarantee shall cease on whichever of the following events first occurs.
    a) Payment by the Bank of the guaranteed sum in full to the 'Employer',

or

b) Receipt of written communication from the 'Employer' to the Bank along with the original Bank Guarantee discharging the Bank of its liability covered by this Bank Guarantee and in case of electronic Bank Guarantee (e-BG), after release/discharge of eBG by the Employer through NeSL Portal.

SIGNATURE AND SEAL OF THE GUARANTOR

DATE: _____

NAME OF THE BANK: _____

ADDRESS: _____

Note:

1. *The stamp paper of appropriate value shall be purchased in the name of the bank, who issues the 'Bank Guarantee".*
2. *The above format shall be used for e-Bank Guarantee also.*
3. *For e-BG, the UIN of BMRCL is 'AAACB4881D'.*
4. *Tender No. shall be the reference to be mentioned in the e-BG.*

PROFORMA – B

FORM OF BANK GUARANTEE FOR PERFORMANCE SECURITY

(Refer GCC clause ……)

(To be stamped in accordance with the Stamp Act of the Country of Issuing Bank)

To
Bangalore Metro Rail Corporation Limited (BMRCL)
3rd Floor, BMTC Complex,
K.H. Road, Shanthinagar
Bengaluru – 560027,
Karnataka, INDIA.

1. **WHEREAS** _____ *[Name and Address of the Contractor]* (hereinafter referred to as the "Contractor") has undertaken for due performance of the Contract, in pursuance of LoA/Contract No. _____ for _____ *[Description of the Contract work to be specified]* (hereinafter referred to as "the Contract"). The Contract was awarded by Bangalore Metro Rail Corporation Limited (hereinafter referred to as the "Employer" or "BMRCL"), which expression shall unless repugnant to the context or the meaning thereof, include its successors, administrators, executors and assignees, to the Contractor.

2. **AND WHEREAS** it has been stipulated in the Contract that the Contractor shall furnish to the Employer with an unconditional and irrevocable Bank Guarantee for *Performance Security* for the sum specified herein below as security for *compliance of the obligations and performance of the Contractor*. In pursuance to this M/s. _____ (the Contractor) has requested for issuance of the Bank Guarantee for the sum specified herein below.

3. **AND WHEREAS we** _____ *[Name and full address of the Bank including Email address]* having registered office at _____ (hereinafter referred to as the "Bank"), which expression shall unless repugnant to the context or the meaning thereof, include its successors, administrators, executors, assignees, and the correspondent Bank hereby agrees to give the Employer on behalf of the Contractor such a Bank Guarantee drawn and payable at Bengaluru branch.

4. **NOW therefore**, the Bank hereby affirm, that it is the guarantor and is responsible to the Employer and their successors, on behalf of the Contractor 'up to a total sum of _____ *[the amount of Guarantee to be specified in figure and words in the respective currency/ies in which the contract price is payable]*. Further, the Bank hereby unconditionally, irrevocably and without demur undertake to immediately pay, the Employer upon the Employer's first written demand and without cavil, or arguments any sum or sums within the limits of the sum specified in this Bank Guarantee as aforesaid without the Employer being required to prove or to show grounds or reasons for the demand, by depositing/crediting to the Current Account of the Employer, the sums specified herein.

5. This Bank Guarantee is encashable at the Issuing Bank's designated Branch in Bengaluru, Karnataka, India as mentioned below:
Name of the Bank, Branch and contact details, Address, telephone no: & Fax No: E-mail Address Branch Manager/s name & Mobile No: Bank Zonal Office Address, Telephone No, Fax Number, E-mail Address: _____

OR

This e- Bank Guarantee shall be encashable at the issuing branch of the Bank through NeSL portal.

6. The Bank hereby confirms that the Bank is on the SFMS (Structural Finance Messaging System) platform and shall invariably send an advice of the Bank Guarantee to the designated Bank of the Employer (Bangalore Metro Rail Corporation Limited) as given below:

Sl. No.	Particulars	Details
i	Name of Beneficiary	Bangalore Metro Rail Corporation Limited
ii	Name of Bank	Bank of India
iii	Branch	Cantonment Branch, Bengaluru.
iv	Address of Branch	49, Jyothi Mahal, St. Mark's Road, Bangalore – 560 001
v	Account No.	840420110000760
vi	IFSC Code:	BKID0008404

7. This Bank Guarantee shall be encashed at the demand of the Employer on or before the due date.

8. The Employer shall have rights to encash this Bank Guarantee at any time during the validity period and the 'Contractor' shall have no right or claim whatsoever in the matter of encashment of the Bank Guarantee amount by the 'Employer'. The Bank will have their responsibility in terms of the guarantee and obligation, to make immediate payment to the 'Employer', without the consent of the 'Contractor' and without referring the matter to the 'Contractor'.

9. The Bank shall be liable to pay the 'Employer', any amount up to and inclusive of the aforementioned full amount upon written order from the 'Employer' to indemnify the 'Employer' for any liability or damage resulting from any defects and/or shortcomings of the 'Contractor' and/or the debts the 'Contractor' may have incurred with the 'Employer' and/or any parties involved in the Works under the Contract mentioned above, whether these defects and/or shortcomings and/or debts are actual and/or estimated and/or expected. The Bank will deliver the money required by the 'Employer' immediately on demand without delay without reference to the 'Contractor' and without the necessity of a previous notice or of judicial or administrative procedures and without it being necessary to prove to the Bank the liability or damages resulting from any defects or shortcomings or debts of the 'Contractor'.

10. Courts at Bengaluru, Karnataka, India shall have exclusive jurisdiction for adjudicating the disputes arising out of the encashment of the Guarantee, and, the said Bank undertakes not to revoke this Guarantee during its currency, except with the previous consent of the 'Employer' in writing and agree that any change in the constitution of the Bank shall not discharge its liability hereunder.

11. This Bank Guarantee will not be discharged due to the change in the constitution of the 'Contractor' or change in the constitution of the Bank.

12. This Deed of guarantee is signed and executed by Shri/Smt _____and Shri/Smt _____who is/are authorized by the Bank for issuing the guarantee on its behalf and their ID No/s. and Email address/es being _____ & _____ and _____ & _____ respectively.

13. The Bank's liability under this Guarantee shall not exceed the amount of_____ *[Indian Rupees/Foreign Currency/ies to be specified in words and figures].*

14. This Bank guarantee shall be valid till _____ *[Date to be mentioned].*

15. The pendency of any dispute or arbitration or other proceedings shall not affect this guarantee in any manner.

16. It is hereby agreed that the liability of the Bank under this guarantee shall cease on the happening of any of the following events:

    a) Payment by the Bank of the Guaranteed sum in full to the 'Employer',

    or

    b) Issue of written communication by the Employer, to the Bank, along with the original Bank Guarantee discharging the Bank of its liability covered by this Bank Guarantee and in case of electronic Bank Guarantee (e-BG), after release/discharge of e-BG by the Employer through NeSL Portal.

SIGNATURE AND SEAL OF THE GUARANTOR

DATE: _____

NAME OF THE BANK: _____

ADDRESS: _____

Notes:

1. *The stamp paper of appropriate value shall be purchased in the name of the bank, who issues the 'Bank Guarantee".*
2. *The Bank Guarantee to be submitted shall be got issued from an Indian Scheduled Bank (excluding Cooperative Bank) or from a Scheduled Foreign Bank as defined in Section 2(e) of RBI Act 1934 read with second schedule.*
3. *The above format shall be used for e-Bank Guarantee also.*
4. *For e-BG, the UIN of BMRCL is 'AAACB4881D'.*
5. *Tender No. shall be the reference to be mentioned in the e-BG.*

--- xxx ----

PAGE INTENTIONALLY LEFT BLANK

SECTION 10 : ANNEXURES

ANNEXURE 1 - FORM OF CONTRACT AGREEMENT

ANNEXURE 2 - CHECKLIST

ANNEXURE 3 – NOT USED

ANNEXURE 4 - FORMAT OF DECLARATION TOWARDS DEBARMENT / BLACKLISTING

ANNEXURE 5 – UNDERTAKING

ANNEXURE 6 - SELF-CERTIFICATION AND DECLARATION FOR LOCAL CONTENT

ANNEXURE 7 - FORM OF CERTIFICATE FOR ELIGIBLE SOURCE COUNTRIES

ANNEXURE- 1

FORM OF CONTRACT AGREEMENT

(To be completed by the Tenderer or by each member in case of JV/ Consortium)

CONTRACT NO. ……..

…….(Name of the Works)……

This Contract Agreement (hereinafter referred to as the "**Contract**") is made at Bengaluru on the___ day of _____ by and between:

BANGALORE METRO RAIL CORPORATION LIMITED, a Public Limited Company incorporated under Companies Act 1956 and a 50:50 Joint venture of Government of India and Government of Karnataka formed for the purposes of execution of a Mass Rapid Transit System in the city of Bengaluru, represented herein by its Company Secretary, authorized to sign and bind the Company, with its registered and corporate office located at III Floor, BMTC Complex (C-Block), K.H. Road, Shanthinagar, Bengaluru 560 027, Karnataka, India hereinafter referred to as the **"BMRCL"** or the **"Employer"**, as the case may be, which expression shall unless excluded by or repugnant to the context or meaning thereof be deemed to include its successors and assigns, of the one part,

and

M/s. ……*(name of the Contractor)*……, a ……..*(legal status)* …….. Company incorporated under Companies Act 1956, having its office at ……..*(Contractor's office address)*……., represented herein by Mr. ……*(name and designation of the representative)*……., authorized to sign and bind the Company under the Power of Attorney dated …… and the Board Resolution dated ……., who shall be responsible to the Employer under the Contract No. …….. for "……..*(Name of the Works)*……", hereinafter referred to as the **"Contractor",** which expression shall unless excluded by or repugnant to the context or meaning thereof be deemed to include its successors and assigns, of the other part.

Hereinafter, **BMRCL**/**Employer** and **Contractor** are collectively referred to as "**Parties**" and individually as "**party**".

WHEREAS, the Employer invited Tenders for Contract No. …….. vide notification no. …….. dated …… and the Contractor has in response submitted a Tender for "……..*(Name of the Works)*……" (hereinafter referred to in this Agreement as **"the Works"**) and agrees to undertake performance of the Works under the terms and conditions set forth in this Contract.

AND WHEREAS, the Contractor emerged as the successful Tenderer and the Employer awarded the Contract to the Contractor and the Contractor agrees for "……..*(Name of the Works)*……" under the terms and conditions specified in this Contract and other Documents, forming part thereof.

NOW THEREFORE THE PARTIES HEREBY AGREE AS FOLLOWS:

Clause 1 Words and Expressions:

In this Contract all the words and expressions shall have the same meaning as are respectively assigned to them in the conditions of Contract hereinafter referred to.

Clause 2 The Contract Documents:

2.1 The following shall be deemed to form and be read and construed as a part of this Contract Agreement.

a) Letter of Acceptance No. …… Dated: ……..

b) The Tender (Bill of Quantities)
c) Instruction to Tenderers/ Bidders
d) General Conditions of Contract
e) Special Conditions of Contract
f) Bid Forms/ Tender Forms
g) Technical Specifications including scope of work
h) Employer's clarifications to Pre-bid Queries and Addendum No….. dated ……..
i) Contractor's 'Qualification cum Technical' and Financial proposals submitted vide letter no. ……. dated ……..
j) All correspondence between the Tenderer/ Bidder and BMRCL from the date of issue of NIT till the date of issue of LOA.
k) Performance Security in the form of Bank Guarantee issued by ……*(name & address of the issuing bank)* ……., vide BG No. …… dated ……. amounting to …….. valid upto …… and its authenticity confirmed by the Bank vide their letter no. …… dated ……
l) Any other document forming part of this Contract.

2.2 All of the foregoing documents, together with this Contract Agreement, are referred to herein as the Contract. Also incorporated into the Contract, and made part hereof, are all codes, standard specifications, and similar requirements that are referred to therein. In the event of a conflict, inconsistency, ambiguity or discrepancy between the contents of the Contract, the order of precedence shall be according to the General Conditions of Contract.

Clause 3 Integration

The Employer and the Contractor agree that this Contract Agreement, together with the other Contract Documents, expresses all of the agreements, understandings, promises, and covenants of the parties and that integrates, combines and supersedes all prior and contemporaneous negotiations, understandings and agreements, whether written or oral and that no modification or alteration of the Contract Documents shall be valid or binding on either party, unless expressed in writing and executed with the same formality as this Contract Agreement, except as may otherwise be specifically provided in the Contract Documents.

Clause 4 Contract Price and Completion Time:

The Contract price is inclusive of all applicable Taxes, Cess and duties under the applicable Acts but exclusive of GST. The GST will be paid as applicable as per law, as per clause 39 of General Conditions of Contract and Special Conditions of Contract) and completion time for executing the works under the Contract are as below:

1.	Estimated Cost specified in the Tender	Rs. ……
2.	Accepted percentage (Tender premium) (Above or Below or At par)	…… % put to Tender.
3.	Accepted Cost of Tender (Tender premium)	Rs……. (Indian Rupees…….only).
Total Contract Price		Rs……. (Indian Rupees…….only).
4.	Date of Commencement of Works	Date of issue of Letter of Acceptance (LOA) as per clause 29 of ITT.
5.	Completion period	…….. as per Appendix to Form of Tender .

Clause 5 Obligations of the Contractor:

The mutual rights and Obligations of the Employer and the Contractor shall be as set forth in the Contract and in particular: -

a) The Contractor agrees, subject to the terms and conditions of the Contract, to perform efficiently and faithfully all of the Works of "……*name of the work*……." under the Contract including ……*(brief scope of works)*…… requisite for or incidental to the successful completion of the Works and in carrying out all duties and obligations imposed by the Contract.

b) The Contractor shall ensure full compliance with Tax laws of India with regard to this Contract and shall be solely responsible for the same. He shall submit copies of acknowledgements evidencing filing of returns and shall keep the Employer fully indemnified against liability of tax, interest, penalty etc, of the Contractor in respect thereof, which may arise.

Clause 6 Obligation of the Employer:

The Employer agrees, subject to the terms and conditions of the Contract to pay Contractor the amount specified and at the rates and terms and in the manner set forth in the Contract.

Clause 7 Governing Law

This Contract shall be construed and enforceable under the applicable laws of the Republic of India. Where recourse to a Court is to be made in respect of any matter, the Court at **Bengaluru** shall have the exclusive jurisdiction to try all disputes between Parties.

Clause 8 Language

This Contract Agreement and other Contract Documents are made in English language.

Clause 9 Notices

All Notices called by the terms of the Contract shall be in writing in English Language and shall be delivered by hand or by registered mail with acknowledgement due. All notices shall be deemed to be duly made by the party to whom it is addressed at the following address or such other address in India as such Party may subsequently
notify to the other.

To Employer:
Bangalore Metro Rail Corporation Ltd.
III Floor, BMTC Complex (C-Block),
K.H. Road, Shantinagar,
Bengaluru – 560 027
KARNATAKA, INDIA.

To Contractor:
.....
.....
.....

Clause 10 Jurisdiction of Court

The Courts at Bengaluru shall have exclusive jurisdiction in respect of all the disputes arising out of this Contract Agreement between the Parties.

IN WITNESS WHEREOF, the Parties hereto have caused this Contract to be signed in their respective names by the hands of their authorized representatives on the day and date first above written.

For **Bangalore Metro Rail Corporation Limited** **(EMPLOYER)**	For **……** **(CONTRACTOR)**
(……..) Company Secretary	(……..)
Witness:	Witness:
(……..)	(……..)

Note:

* *This Contract Agreement form may be modified as considered necessary at the time of finalisation /signing of the Contract Agreement.*

** *Blanks to be filled by the BMRCL at the time of finalization of the Form of Agreement.*

*** *Any other condition considered to be essential in the interest of BMRCL shall be included.*

ANNEXURE - 2

CHECK LIST**

(A) The following check list is intended to help the Tenderers in submitting offer which are complete. An incomplete offer is liable to be rejected. Tenderers are advised to go through the Tender documents and the list carefully and take necessary action.

(B) Tenderers are also required to submit copy of the checklist, duly marked, along with their offer. The Tender submittals shall consist of the following:

I	**QUALIFICATION CUM TECHNICAL PACKAGE**	
a.	Earnest Money Deposit (Clause 14 of ITT)	Submitted / Not Submitted
b.	Form of Tender on firm's Letter head (Clause 10 of ITT)	Submitted / Not Submitted
c.	Notarized Power of Attorney (Clause 15.2 / 16.1 of ITT) / Attested copy of the Partnership deed / Ownership record to demonstrate the authority to sign the Tender submittals.	Submitted / Not Submitted
d.	Evidence of 'Tenderer's Eligibility and Qualification Criteria (Clause 2 & 3 of ITT) and **Qualification Information** (Section 3) with CA's certifications.	Submitted / Not Submitted
e.	Copy of PAN card	Submitted / Not Submitted
f.	Copy of GST Registration certificate	Submitted / Not Submitted
g.	**Undertakings** as per prescribed Proforma given in **Annexure-4** & **Annexure-5 in Section-10.**	Submitted / Not Submitted
h.	Self-certification and details of local value addition as per Annexure-6 and Attachment to Annexure-6	Submitted / Not Submitted
i.	Constitution or legal status of Tenderer as per clause 1.1 of Section 3.	Submitted / Not Submitted
j.	List of works executed and payments received year wise in the last five years as per clause 1.2 of Section 3 duly certified by CA**.**	Submitted / Not Submitted
k.	Existing commitments and ongoing works as per clause 1.3 A of Section 3.	Submitted / Not Submitted
l.	Works for which Tenders already submitted as per clause 1.3 B of Section 3.	Submitted / Not Submitted
II	**FINCANCIAL PACKAGE**	
a.	'Pricing document (Bill of Quantities)' through eProcurement Portal as per Instructions for completing the Pricing Document, Section-XI and ITT Clause 10 of ITT.	Submitted / Not Submitted

Note to the Tenderer:

*** - The above list is not exhaustive, any other document/s which are required as per the Tender document shall be submitted.*

Note to the TIA:

 # - If any other documents are required, the same shall be listed.

ANNEXURE - 3

Not used

ANNEXURE - 4

FORMAT OF DECLARATION TOWARDS DEBARMENT / BLACKLISTING

(To be completed by the Tenderer or by each member in case of JV/ Consortium)

We, M/s. ..... *[Name of the Tenderer]*…… (hereinafter called the "Contractor"), do hereby affirm and declare that we have NOT been Black listed / Debarred by any Government / Government undertaking / semi Government / Govt. Controlled Institutions/projects in India, during the last five (5) years*.

We have not rescinded the Works after award of the Contract during the last five (5) years*.

In case it is found that above statement is not true, any time during effect of this Tender or currency of the Contract entered between the parties based on the above statement, BMRCL reserves its rights to terminate the Contract and forfeit the Tender Security / Performance Security at its discretion.

Place: Signature of the Tenderer

Date: Name

Designation

Seal of the Company

*Note: * Last five (5) years shall be counted from 28 days prior to the date of submission of the Tender.*

ANNEXURE - 5

UNDERTAKING

We, M/s..... *[Name of the Tenderer]……,* herein after called “the Contractor”, do hereby affirm and undertake to abide by all the terms, conditions and specifications given in the Tender document while performing the contractual obligations relating to …….*[name of work]……..* of BMRCL, Bengaluru.

We do hereby affirm and undertake to follow all labour laws that are applicable from time to time.

We also undertake that the Tender submittals do not contain any deviation or amendment or modification or change of any type whatsoever with regard to tender conditions and specifications.

Place: Signature of the Tenderer

Date: Name

Designation

Seal of the Company

ANNEXURE -6

FORM OF SELF-CERTIFICATION AND DECLARATION FOR LOCAL CONTENT

I/We.....(jointly and severally) declare that I/we have offered this Tender with the local content of .....% and has given "details of the locations(s) at which the local value addition is made" as per Table-A & B of Attachment to this Annexure.

I/We declare that the Local Content of ……% mentioned above, is excluding the Services such as transportation, insurance, installation, commissioning, training and after sales services support like AMC/CAMC etc., in line with OM No. P-45021/102/2019-BE-II-Part (1) (E-50310) dated 04.03.2021.

I/we further declare that the Imported items sourced locally from resellers/distributors are also excluded from the calculations of 'Local Content' as detailed in Table C of Attachment to this Annexure.

I/We further acknowledge the right of the Employer to impose a penalty up to 10% of the Contract Price, in case the Contractor does not meet the stipulated Local Content requirement and the category of the Contractor changes from Class-I to Class-II/ Non-local or from Class-II to Non-local.

I/We further acknowledge the right of the Employer to debar the Tenderer for any violation or false declaration, regarding 'Local content' or local value addition (including payments to be made to their vendors for local value addition), which shall be treated as fraudulent practice under ITT Clause 34.3 of this Tender for which the Tenderer or its successors can be debarred for up to two (2) years as per Rule 151 (iii) of the General Financial Rules along with such other actions as may be permissible under law

SIGNATURE OF THE TENDERER

Note:
Please refer GCC Clause 1.1(ee) for definition and valuation of "Local Content" and MoHUA Office Memorandum/s

ATTACHMENT TO ANNEXURE-6

TABLE-A PROPOSAL FOR SYSTEMS/SERVICES TO BE DEVELOPED/ SUBCONTRACTED IN INDIA

INFORMATION TO BE FURNISHED BY THE TENDERER FOR SERVICES TO BE PROCURED / SUBCONTRACTED / SOURCED IN INDIA							
Sl. No.	Equipment/ Sub-systems/ Services	To be Produced/developed in India by the Tenderer			To be produced by the Tenderer from vendors/Subcontractors in India		
		Percentage (%)	Description	Address	Percentage (%)	Description	Address
1							
2							
…							

TABLE-B PROPOSAL FOR SYSTEMS/SERVICES TO BE SOURCED OUTSIDE INDIA

INFORMATION TO BE FURNISHED BY THE TENDERER FOR SERVICES TO BE SOURCED OUTSIDE INDIA					
Sl. No.	Equipment/ Sub-systems/ Services	To be sourced from outside India			
		Country of Origin	Percentage (%)	Description	Address

TABLE-C: PROPOSALS FOR IMPORTED ITEMS (EQUIPMENT/SUB-SYSTEMS/SERVICES) TO BE SOURCED FROM RESELLERS/ DISTRIBUTORS IN INDIA

Information to be furnished by the Tenderer for Imported Items (Equipment/Sub-Systems/Services) to be sourced from Resellers/ distributors in India										
Sl. No.	Equipment/ Sub-systems/ Services	Imported Items to be sourced from Resellers/distributors in India								
		Country of Origin	Cost						Description of firm	Address
			Cost of Item	Taxes	License Fee	royalties paid	Technical expertise	Any other		

Note: Item wise details of Imported Items to be sourced from Resellers/ distributors in India shall be specified by the Tenderer.

SIGNATURE OF THE TENDERER

ANNEXURE -7

FORM OF CERTIFICATE FOR ELIGIBLE SOURCE COUNTRIES

(To be submitted on Tenderer's Letter head)

1. I/We *.....(Name of the Tenderer/Member).....*.have read ITT clause 35 regarding restrictions on procurement from a Tenderer of a country which shares a land border with India and on subcontracting to contractors from such countries; and I/we certify that I/we am/are:
   a) **not from such a country,*

   or,

   b) **from such a country (.....indicate country.....), have been registered with the Competent Authority[@],*

   and will not **subcontract** any work to a contractor from such countries unless such contractor is registered with the "Competent Authority".

   I/We hereby certify that I/we am/are fulfilling all requirements in this regard and eligible to be considered, in accordance to ITT clause 35.

2. I/We have read the ITT clause 35 regarding restrictions on procurement from a Tenderer having Transfer of Technology (ToT) arrangement. I/We certify that this Tenderer:
   a) **does not have any ToT arrangement requiring registration with the "Competent Authority"**

   OR

   b) **has valid registration to participate in this Tender[@].*

3. *1/We submit a registration certificate herewith as an evidence of valid registration by the "Competent Authority" and I/We further acknowledge the right of the Employer that absence of such a registration certificate in the Tender, if the Tenderer belongs to such country stated above, shall disqualify the Tenderer.

4. I/We acknowledge the right of the Employer to terminate the Tenderer for false declaration or certificate, along with further legal action in accordance with law.

SIGNATURE OF THE TENDERER

Note:
** Delete whichever is not applicable.*
[@] Evidence of valid registration by the Competent Authority shall be attached.

--- xxx ----

SECTION 11

INSTRUCTIONS FOR COMPLETING THE PRICING DOCUMENT

1) The Tenderer shall fill in and complete the Bill of Quantities (Financial Package) online through Karnataka Public Procurement Portal (eProcurement portal) only and **no hardcopy of commercials should be attached or disclosed anywhere in the technical Package.**

2) The Tenderer shall quote the rates & amount in the 'Pricing Document (Bill of Quantity)' given in the Karnataka Public Procurement Portal.

3) The total Tender price shall be inclusive of all applicable Taxes duties & cess under the applicable Acts but **exclusive of GST**. BMRCL shall pay the applicable GST as invoiced by the Contractor to BMRCL.

4) The Tenderer shall ascertain all applicable Taxes Duties & cess under the applicable Acts and shall be included in the quoted price.

5) The evaluation and comparison of Tenders shall be made accordingly by BMRCL. No claim will be entertained on this account after acceptance of the Tender or during the currency of the Contract.

6) **Income Tax (IT) deduction:** As per the prevailing rate, IT shall be deducted and remitted to the Income Tax authorities and Form 16 shall be furnished by BMRCL in proof of remittance to IT Department for availing lower deduction of Income Tax, necessary certificate for each financial year issued by the Income Tax Authority shall be furnished by the Contractor, failing which IT at the maximum rate will be deducted.

7) The Cost of all the individual items shall be computed for the entire work and the rates and amount on the Total (Estimated) cost shall be quoted. Any additional item/s not found in the BOQ and if it is required to be executed for completion of the work under this Contract, the rate for which shall be as per KPWD schedule of Rates of the respective year above or below Tender premium which the BMRCL has accepted. If the item required is not found in any of the schedule of Rates of KPWD or CPWD, then rate shall be worked out as stipulated in GCC Clause 34.

8) The Prices quoted by the Tenderer shall be fixed for the duration of the Contract and shall not be subject to adjustment on any account.

9) Tender submitted with an adjustable price quotation will be treated as non-responsive and rejected, pursuant to ITT Clause 23.

10) The Tender Price shall be inclusive of all charges of insurance, transportation up to destination, handling, installation, royalties & any other charges leviable and payable by the Contractor under the Contract, or for any other cause and including Tax to be deducted at source and shall be included in the Total Tender Price.

11) The Contractor shall be entirely responsible for license fees and any other incidentals incurred until completion of the whole of the Works and handover to the Employer.

12) The Contractor shall maintain complete records of duties, other taxes and levies etc. payable to various authorities in relation to the Works and submit the receipts/records for verification as and when demanded in writing by the Employer.

13) Any increase in GST shall not be paid in the extended period of Contract for which the Contractor alone is responsible for delay as determined by the Engineer while granting the Extension of Time. However, this shall not be applicable for "Variations".

14) UNPRICED ITEMS: Items against which no rate or sum is entered in the Bill of Quantities, whether quantities are stated or not shall be regarded as covered by other rates in the Pricing document. The Tenderer shall take regard of the actual site conditions and the items entered in the Bill of Quantities. The Tenderer shall price his Tender accordingly and the rates and amount in the BOQ shall be full and only price paid for all work performed against that item except as described in the Tender Documents.

15) BMRCL will consider only the prices quoted in the pricing document for evaluation of Tender.

16) The cost quoted for CAMC & 'Operation of SOC' will be paid in equated quarters as per Pricing document.

--- XXX ---

SECTION 12

PRICING DOCUMENT (BILL OF QUANTITY)

Sl. No	Description of item (with brief specification and reference to specification)	Quantity	Unit	Rate (INR)	Amount (INR)
Schedule-I – Establishment of SOC					
1	Supply, Installation, Testing, Integration & Commissioning of following systems/application including, warranty for 1 year from Go-Live.	-	-		
1.1	SIEM,SOAR/SOC Security platform : SOC ecosystem with integrated SIEM, Threat Intel, Compliance reporting and File Integrity Monitoring, Security Configuration Assessment, Anomaly detection and Vulnerability management; for Firewalls, Critical Servers or Networking devices covering the Critical devices. devices covering the devices.	-	-		
	a) SIEM	1	Set		
	b) SOAR	1	Set		
	c) SOC	1	Set		
	d) UEBA	1	Set		
	e) NOC (CCTV Network)	1	Set		
1.2	85” LCD Display	1	No.		
1.3	Workstation with dual monitor	4	Nos.		
Sub-total of Schedule-I					
Schedule-II – CAMC & Operation					
A.	**Comprehensive Annual Maintenance Contract (CAMC) for whole SOC System for 3 years from completion of warranty including spares, license fees.**				
1	SIEM, SOAR, UEBA & SOC Platform	3	years		
2	NOC (CCTV NETWORK)	3	years		
3	85” LCD Display	3	years		
4	Work station with dual monitor	3	years		
B.	**Operation of SOC for 3 years from Go-live**				
5	Operation cost for 3 years including manpower with Level-3 support				
5.1	For 1st year	1	year		
5.2	For 2nd year	1	year		
5.3	For 3rd year	1	year		
Sub-total of Schedule-II					
TOTAL OF SCHEDULE-I & II					